

MASS. G68.8. C713 / C13

UMASS/AMHERST



312066016807653

COMPUTER CRIME LAWS: A REPORT TO THE GOVERNOR

GOVERNMENT DOCUMENTS
COLLECTION

1994

University of Massachusetts
Depository Copy

MASSACHUSETTS COMMISSION ON COMPUTER TECHNOLOGY AND LAW
FEBRUARY 1, 1993

942 / 299

Massachusetts Commission on Computer Technology and Law

Commission Members

Brian Carty
Coopers & Lybrand

Joseph DeNucci
State Auditor
Office of the State Auditor

Jack Doherty
Public Affairs/Corporate Communications
New England Telephone

William Dudley
A. G. Edwards & Sons, Inc.

J. Thomas Franklin
Lucash, Gesmer, and Updegrove
Massachusetts Bar Association

Sally Greenberg
Civil Rights Counsel
Anti-Defamation League

Paul D. Harold
Chair, Joint Committee on Criminal Justice

Scott Harshbarger
Attorney General
Office of the Attorney General

Richard Hurley
Chief of Police
Medfield Police Department

Mitchell Kapor,
Commission Chairman
President, Electronic Frontier Foundation

John LeBaron
University of Massachusetts at Lowell and the
Massachusetts Education Computer Network

Joseph McIntyre
House Chair
Joint Committee on Criminal Justice

Robert McKenna
Suffolk County District Attorney's Office

Gregory Moore
Ropes & Gray
Boston Bar Association

William O'Malley
District Attorney
Office of the Plymouth County District Attorney

Joyce Plotkin
Executive Director
Massachusetts Computer Software Council Inc.

Ron Reiling
Mass High Tech Council

Francis D. Riley
Bureau of Investigative Services
Department of the State Police

James P. Shaughnessy
Law Department
Digital Equipment Corporation

Steve Tocco
Secretary for Economic Affairs
Office of Economic Affairs

Designees

Joseph Alexander
Development Coordinator
Massachusetts Office of Business Development

Edward D. Rapacki
Assistant Attorney General
Office of the Attorney General

John Beveridge
Deputy State Auditor - MIS/EDP Audit
Office of the State Auditor

Mark Seligman
Coopers & Lybrand

Other Contributors

Regina Blaney
Office Manager
Electronic Frontier Foundation

Patrick Halley
Director of Operations
Office of the Attorney General

Brett C. J. Britton
Research Assistant
Electronic Frontier Foundation

Ann Marie Irwin
Legal Counsel
Joint Committee on Criminal Justice

Thomas Ericson
EDP Audit Manager
Office of the State Auditor

Sergeant Andrew Palombo
Office of the Attorney General

Michael Godwin
Chairman of the Drafting Committee
General Counsel
Electronic Frontier Foundation

Todd Shapiro
Research and Policy Analyst
Joint Committee on Criminal Justice

Mark Hagan
EDP Auditor
Office of the State Auditor

Acknowledgements

The Commission on Computer Technology and Law wishes to thank the Electronic Frontier Foundation for providing staff support, research help and coordinating the printing of this report. The Commission also wishes to thank Ropes & Gray for hosting the Commission meetings, and providing administrative and research help.

Special thanks to Alameda County Assistant Attorney General Don Ingraham for traveling to Boston for his presentation on the California comprehensive computer-related crime statute. Mr. Ingraham provided information and insights into the pros and cons of the comprehensive legislative approach to computer-related crimes. His experience and comments were valuable in developing the legislative approach adopted by the Commission.

TABLE OF CONTENTS

Commission Members.....	i
EXECUTIVE SUMMARY.....	v
Introduction and overview	1
Threshold issues	1
Summary of Commission recommendations	2
The First Amendment and computer forums.....	3
The choice between a comprehensive statute and the incremental approach.....	4
Recommendations of the Commission	6
Extending criminal trespass to cover computer intrusion	6
Extending the vandalism prohibition to cover alteration or destruction of electronic information.....	7
Theft of computer services	8
Modernizing the Best Evidence Rule to allow admission of duplicates of computer files..	11
Suggestions considered and rejected by the Commission.....	14
The role of education in addressing and deterring computer crime	16
Appendix A	19
Appendix B.....	30
Appendix C.....	33
Appendix D	36
Appendix E.....	47

EXECUTIVE SUMMARY

Pursuant to Executive Order #322, the Commission on Computer Technology and Law reports on its consideration of the issues and interests raised by the problem of computer crime in Massachusetts.

A threshold question for the Commission was: What computer-related conduct, if any, that is not already reachable under current Massachusetts criminal law, or under federal law, should be criminalized? The Commission found that much of what is labeled "computer crime", e.g., theft of funds through manipulation of computer accounts, would be crime even without a computer. In the Commission's view, only a few areas require legislative action.

Research into the state of computer crime in Massachusetts revealed that mere computer intrusion, without damage, seems not to be addressed by current Massachusetts law, nor do the Commonwealth's vandalism and theft-of-services statutes address the potential for computer intruders to intentionally damage systems or data, or to make use of commercial computer services without paying for them.

The Commission addressed concerns about the harmful effects on business of computer intrusions and snooping, theft of information, and damage to data. The Commission felt strongly that any new criminal laws be linked to specific behavior and intent, not simply to the use of a computer or computer network. Other expressed concerns were: privacy and the protection of personal information, First and Fourth Amendments rights, copyright and intellectual property issues, the contamination or destruction of data, use of computers in fraud, computer "viruses" and other destructive computer programs, and theft of services.

Recommendations

Once the Commission determined that some changes in Massachusetts law were appropriate, it decided that this should occur through additions to existing Massachusetts criminal provisions, rather than by drafting a comprehensive computer crime statute. The Commission believes that modifying existing law, and thereby building upon existing, familiar legal principals, will better protect the interests of both society and criminal defendants. The approach should allow courts and lawyers to build on existing precedent and procedures, thereby providing more certainty of result.

Specifically, the Commission recommends that the Commonwealth: adopt a statute penalizing computer "trespass"; criminalize the vandalism of computer systems or data; create a theft-of-services statute applying to theft of commercial computer services; and expand Massachusetts evidence law to allow for the admissibility of copies and printouts of computer files.

The Commission also has concluded that education will be the key element of an integrated strategy for: preserving civil liberties; ensuring law-enforcement efficiency in computer crime investigations; encouraging compliance with the law; and informing policymakers of the need for new law.

Criminal Trespass

The Commission recommends extending existing criminal trespass law to cover computer intrusion that the intruder knows to be unauthorized.

The Commission bases its recommendation on the premise that the unauthorized access of a computer system is wrong, and should be illegal. The Commission believes that its suggested amendment of the criminal trespass law articulates clearly that mere unauthorized access to a computer or computer system, even without an intention to do further wrong, should be discouraged and punished.

Vandalism

The Commission recommends extending the Commonwealth's existing vandalism statute to cover alteration or destruction of electronic information.

The Commission proposes that the definition of personal property subject to prosecution for intentional alteration, damage or destruction be broadened to include electronic data. This amendment would not change in any way the elements of the crime or the proof to which the Commonwealth is held. The amendment would reflect society's commonly shared dependence upon the integrity of information that dictates human events.

Theft of Services

The Commission recommends that Massachusetts' "theft of service" law be expanded to include the theft of service from commercial on-line computer services.

The Commission believes that this should be limited to computer service and data that are commercially available, as opposed to private systems. This distinction is based on the Commission's view that commercial systems would not be protected adequately by a computer trespass statute.

Rules of Evidence

The Commission recommends that the legislature and courts of Massachusetts take appropriate steps to adopt the Federal Rules of Evidence provisions regarding the definitions and admissibility of "originals" and "duplicates" of computer data. The Commission believes that modernizing Massachusetts evidence law in this way would both minimize the intrusiveness of searches and seizures of computers and increase the efficiency of criminal investigations that require the gathering of computer evidence.

Education

Education of the public will be a critical component of implementing effectively the legislation recommended by the Commission. Such education should be integrated into a continuum of industry standards, practices and ethics.

Education of the law enforcement community is equally essential due to the rapidity of change within the industry. Finally, expedited communication between the industry and the law enforcement community will enhance enforcement and increase sensitivity to private sector concerns. Coordination, direction and supervision of this educational function should be committed to the Attorney General.

The Commission believes that these legislative changes will improve the Commonwealth's ability to respond to computer crime while protecting and preserving the legitimate interests of computer owners and users.

Section I

Introduction and overview

A. *Threshold issues*

What computer-related conduct, if any, that is not already reachable under current Massachusetts criminal law, or under federal law, should be criminalized? This was the major issue before the Commission.

At the outset, several of the Commissioners, including representatives of law enforcement, noted that there was an increased use of computers and computer networks in traditional crimes. Although the law-enforcement representatives believed that existing statutes reach these traditional crimes whether computers are used or not, they also believed that some changes in the law to reflect the increased use of computers may be helpful. There was a consensus among the Commissioners, however, that the nature of traditional crimes is not changed merely because a computer is used to commit the crime, and that computers should be viewed more as neutral instruments of these crimes, rather than as an important element. In the words of one Commissioner, a computer used in a crime is more like a car used for a getaway than like a gun used to commit a robbery.

There was also a sense that computers had spawned new conduct that society should seek to deter and punish. Several Commissioners expressed concern about the harmful effects on business and society of computer intrusions and snooping, theft of information, and damage to data; if current law did not adequately deter such conduct, these Commissioners believed, it should be amended to do so. There was a consensus among the Commissioners that certain norms of permissible conduct could be laid down, and that it was important to make these norms clear and understandable in order to give people clear guidance in the conduct of their affairs. The Commission feels strongly that any new criminal laws be linked to specific harmful behavior and intent, not simply to the use of a computer or computer network or the dissemination of information.

Among the other concerns expressed throughout the Commission's meetings were: privacy and the protection of personal information, First and Fourth Amendment rights, copyright and intellectual property issues, the contamination or destruction of data, use of computers in fraud, computer "viruses" and other destructive computer programs, and theft of services.

The Commission held a total of seven meetings over the period July, 1992 through January 1993. At several of these meetings, presentations were made to the Commission by Commissioners and others on the problems faced by businesses and other organizations, on existing Massachusetts law, on Federal law relating to computer crime, on the approaches taken by other states, and on the practical problems faced by law enforcement agencies in trying to deal with crimes involving computers. The Commission did not hold public hearings in formulating its report and recommendations, in the expectation that public hearings will be part of any legislative consideration of this report.

A discussion of the laws among the various states appears in a National Institute of Justice report included here as Appendix A, and an outline of state-law computer-crime provisions appears as Appendix B. The federal Computer Fraud and Abuse Act, 18 USC §1030, appears as Appendix C, but it should be noted that other, more general, federal laws are routinely used in federal computer-crime prosecutions. These federal laws include the wire-

fraud statute (18 USC §1343), the interstate-transportation-of-stolen-property statute (18 USC §2314), the statute barring unauthorized trafficking and use of "access devices" (18 USC §1029), the Wiretap Act (18 USC §2510 et seq.), and the stored-communications chapter of the Electronic Communications Privacy Act (18 USC §2701 et seq.). Prosecutors' use of these federal statutes in computer-crime cases is also discussed in Appendix A.

Research into the state of computer crime in Massachusetts led to a number of preliminary findings:

- Mere computer intrusion, without damage, seems not to be addressed by current Massachusetts law, nor do the Commonwealth's vandalism and theft-of-services statutes address the potential for computer intruders to intentionally damage systems or data, or to make use of commercial computer services without paying for them
- These non-traditional acts of computer wrongdoing appear to be neither a complete non-issue nor a major, widespread problem. It was felt that as computer use increases, and computer literacy becomes more widespread, inappropriate computer conduct will probably increase.
- There do not seem to be many cases in Massachusetts or other jurisdictions in which a lack of specific law relating to the use of computers in traditional crimes has left law enforcement seriously unable to prosecute these offenses.¹

Based upon these findings, the Commission concluded that it should consider legislation directed at computer trespass, destruction of computer data, and theft of computer services.

B. *Summary of Commission recommendations*

Once the Commission determined that some changes in Massachusetts law would be appropriate, a second question was raised: If new criminal sanctions for computer-related conduct are to be enacted, should this occur through additions to existing Massachusetts criminal provisions, or should it occur by drafting a comprehensive computer-crime statute? The commission recommends the former strategy, for reasons discussed in Section II below.

The specific suggestions for changes in substantive criminal law are discussed in Section III. These include expanding the criminal trespass statute to cover computer trespass, expanding the definition of property subject to the vandalism prohibition of the Commonwealth's personalty statute, expanding the reach of theft of service laws to cover theft of commercial computer services, and modifying the rules of evidence to deal better with computer records.

The Commission also considered several other issues and specifically concluded, and recommends, that these not be addressed at this time through the criminal laws. These issues include extension of the larceny statute to cover all data, theft of non-commercial computer services, denial of service and penalties for inadequate security. The reasons for the Commission's conclusions on these issues are set forth in Section IV.

¹ In the National Institute of Justice report "State Computer Crime Statutes" (Research in Action, November 1991, reprinted as Appendix A in this report), author Hugh Nugent states that "[d]espite some ingenious defense arguments, most courts and prosecutors had little difficulty applying traditional concepts to computer offenses."

The Commission also has concluded that education will be a key element of an integrated strategy for a) preserving civil liberties b) ensuring law-enforcement efficiency in computer-crime investigations, c) encouraging compliance with the law, and d) informing policymakers of the need for new law. The Commission offers recommendations for educational initiatives in Section V.

As is evident from a review of the list of Commission members included elsewhere in this Report, the Commission was composed of people representing many different organizations and constituencies, who brought to the Commission very different perspectives on the issues before the Commission. These included private businesses, educational institutions, civil liberties organizations, the private bar and law enforcement organizations. Despite these differences, the Commission quickly developed a consensus on the issues, and on the recommendations included in this Report.

C. *The First Amendment and computer forums*

New computer-based forums for debate and information exchange are facilitating perhaps the greatest exercise of freedom of expression that the United States, and the rest of the world, has ever seen. In addition, far-flung computer networks are making it possible to disseminate new discoveries and other news to any place on Earth almost instantaneously, and are allowing people and business to communicate efficiently and economically across time zones, continents and oceans. The computer's role as an instrument of communication may be more important than any other role. The Commission believes it is critical, therefore, that policymakers neither criminalize behavior that is arguably protected by the First Amendment, nor pass laws that suggest that there is something illegitimate or dangerous about communicating via computer.²

² The simplest computer forum is the electronic bulletin-board system (BBS). The operator of a BBS typically dedicates a computer and one or more phone lines at his or her home or business for the use of a "virtual community" of users. A user may call up the BBS and leave public messages that can be read by all other users, or private mail that can be read by a particular user, or both. BBSs become forums--digital public houses, salons, and Hyde Park corners--for their users, and users with similar interests can associate with one another without being hindered by the accidents of geography.

A step up from the BBS in complexity is the conferencing system or information service. Like BBSs, these systems are typically based on a single computer or set of computers located in a particular geographic area. They differ from BBSs in capacity: they have the capability of serving dozens, or hundreds, of users at the same time. CompuServe of Columbus, Ohio, and the WELL (Whole Earth 'Lectronic Link) of Sausalito, California are two of the better-known examples of such systems.

"The WELL ... is an example of the latest thing in frontier villages, the computer bulletin board. In this kind of small town, Main Street is a minicomputer to which ... as many as 64 microcomputers may be connected at one time by phone lines and ... modems....

"There are thousands of these nodes in the United States, ranging from PC clone hamlets of a few users to mainframe metros like CompuServe, with its 550,000 subscribers. They are used by corporations to transmit memoranda and spreadsheets, universities to disseminate research, and a multitude of factions, from apiarists to Zoroastrians, for purposes unique to each.

"Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net." J. Barlow, "Crime and Puzzlement," Whole Earth Review, Fall 1990, pp. 44-57.

Still further up the scale in complexity is the distributed network, which is not located in a particular geographic area but is maintained and supported on a large number of computers located all over the country (or the world).

Legal commentators routinely regard computer networks and computer forums as deserving of First Amendment protection.³ Moreover, the United States Supreme Court has articulated a fairly broad definition of the "the press" for the purposes of interpreting the First Amendment's Press Clause. The Court has held that "[t]he liberty of the press is not confined to newspapers and periodicals. It necessarily embraces pamphlets and leaflets.... The press in its historic connotation comprehends every sort of publication which affords a vehicle of information and opinion" (*Lovell v. City of Griffin*, 1938). Freedom of the press, the Court has said, includes "the right of the lonely pamphleteer who uses carbon paper or a mimeograph as much as of the large metropolitan publisher who utilizes the latest photocomposition methods" (*Branzburg v. Hayes*, 1972). The main difference between users of the new computer communications media and "the lonely pamphleteer" is that technology has made the former much less lonely.

But like all new technologies that transform the way we live, computers have gone through a period of social mistrust and fear, often expressed in articles, books, and films. It is easy to forget, in the face of speculations about the threats posed by this new technology, that computers also have great potential for enhancing the freedoms of speech, publication, and association in a free society. The Commission believes it is vital, during this period of social transition, that the Commonwealth not risk seeming to characterize use of computers for these purposes as socially marginal or quasi-criminal. For these reasons, the Commission was very sensitive in its deliberations to First Amendment interests and has taken care in its recommendations to protect these interests.

Section II

The choice between a comprehensive statute and the incremental approach

In examining the responses of other states to the issue of Computer Crime, the Commission found two very different approaches.

Most of the other states that have grappled with computer crime issues have chosen to enact comprehensive, stand-alone statutes that focus specifically and exclusively on computer-related activities. Two examples, the revised California statute and the New Mexico statute, are included as Appendix D to this Report.

The best-known example of a distributed network is the Internet, which directly connects thousands of computers at universities, government entities, and commercial and noncommercial organizations around the world with one another. Hundreds of other computers gain access to Internet-connected systems via dialup telephone lines. Together, this vast system of interconnected computers is often called "the Net," and its public conferencing system ("Usenet") and electronic-mail services have enabled hundreds of "virtual communities" of like-minded individuals to spring up. The largest computer network in the United States, the Internet, is actually made up of 2,000 smaller networks. See, e.g., "Common Electronic Policy," *The Economist*, Feb. 16, 1991, at 24. The Internet reportedly carries the electromagnetic impulses created by over 500 billion keystrokes per month. See Leccese, "Hackers under Attack: Crackdown Raises Questions about New Forms of Speech," *Boston Phoenix*, Sept. 7, 1990. The immediacy of electronic mail and Usenet has already led to their supplanting of scientific journals as the major communicators of new scientific discovery and research. See "Common Electronic Policy," *The Economist*, Feb. 16, 1991, at 24.

³ See generally, Jensen, *An Electronic Soap Box: Computer Bulletin Boards and the First Amendment*, 39 *Fed.Communications L.J.* 217, 235P43, and authorities cited therein.

A minority of the states have chosen to modify existing criminal statutes to expressly include various computer related activities. An example of one of these, Ohio's response, is included as Appendix E to this Report.

The Commission gave considered thought to the choice between these two approaches. Many members of the Commission began with a preference for an incremental approach. Others had no initial preference. During the course of the Commission's meetings it received a presentation by California Assistant District Attorney Don Ingraham on the history of the California statute and its use in the courts.

After considering both alternatives, the members of the Commission are unanimous in preferring, and recommending, an incremental approach that makes modifications to existing Massachusetts law. As discussed below, the Commission has identified three areas where existing law does not reach conduct that the Commission believes most people would agree should be reached. It believes that relatively minor changes to a handful of existing statutory provisions will adequately address these areas.

The Commission believes that modifying existing law, and thereby building upon existing, familiar legal principles, will better protect the interests of both society and criminal defendants. The approach should allow courts and lawyers to build on existing precedent and procedures, thereby providing more certainty of result. This is the approach followed by the Legislature when it amended the general larceny statute (c.266 §30) to include intangible data as property, and when it amended the statute relating to theft of telecommunications service (c.166 §42A) to include theft of cable television service, to cite only two examples.

In contrast, the Commission believes that any attempt to address computer crime through new, comprehensive, legislation risks fostering uncertainty. These new statutes typically contain new definitions that will have to be tested in court before their meanings are really known. These same definitions may also serve to freeze today's problems and today's technology into laws that will need to be used tomorrow. The Commission also believes that this approach makes it harder to bring well-established principles of law to bear on computer crime.

At bottom, the Commission believes that the fundamental wrong involved in most, if not all, computer crime is more closely related to the crime than the computer. If conduct is wrong when a computer is involved, it is probably also wrong if done without a computer. There are of course wrongs that, by their nature, wouldn't have existed without computers, for example destruction of programs or theft of computer service. However, the Commission believes that these wrongs are similar enough to existing crimes, for example, vandalism of personal property or theft of cable television service, that they can be easily accommodated in the incremental approach.

The Commission also believes, that the magnitude of the computer crime problem is not as great as might be inferred from the coverage that the issue has received in the popular media. This is not to say that the problem is not real, or that it is not a serious threat to businesses, governments and people: it is both. However, the Commission believes that modifying existing law is a more proportionate response to the problem than creating a new, comprehensive statutory scheme.

Finally, if the Commission is wrong, and the approach recommended by it proves unequal to the problem, a comprehensive approach can again be considered. If, on the other hand, a comprehensive approach were tried first, it would be difficult, if not impossible, to return to an incremental model.

Section III

The Recommendations of the Commission

A. *Extending criminal trespass to cover computer intrusion*

The Commission recommends the addition of a new §120E to c.266 of the Massachusetts General laws:

COMPUTER TRESPASS

Whoever, without right, gains unauthorized electronic access to a computer system, whether by telephone or computer-network connection or by direct physical contact with a computer terminal or other device attached to the computer system, and

- a) knows that such access is unauthorized; or
- b) learns, directly or indirectly, after gaining such access that such access is not authorized and who fails to terminate such access;

shall be punished by a fine of not more than one thousand dollars or by imprisonment for not more than thirty days in the house of correction, or both.

The requirement of a password or other user authentication to gain access shall constitute notice that access is limited to authorized users.

Discussion of proposed amendment

At present, unauthorized access to a computer or computer system is not a violation of Massachusetts law. This is true whether the access is accomplished using telephone communications or physically from the premises which contain the computer.

The Commission bases its recommendation for an addition to Massachusetts criminal-trespass law on the premise that the unauthorized access of a computer system is wrong, and should be illegal. Although computer enthusiasts of an earlier era may have argued that tolerance for unauthorized computer access may serve a useful purpose⁴, there is a strong consensus among the members of the Commission that the potential risks of harm caused by computer intrusion merit a law that deters such intrusion. Moreover, the Commission was specifically directed to consider privacy issues, and, even if no other harm is done, unauthorized access is an invasion of an expectation of privacy--an expectation that should

⁴ See, e.g., Hackers: Heroes of the Computer Revolution, by Steven Levy, pp. 39-49. Dell Books, 1985.

be protected. The Commission believes that extension of the law of trespass to computer systems is an appropriate way to do this.

Moreover, if, as Robert Frost noted, "good fences make good neighbors," it follows that any computer trespass law should give owners of computers that can be accessed via telephone or network connection an incentive to give notice to potential trespassers that access is limited. The Commission believes that the requirement of a password or other user authentication can reasonably be taken as notice to potential trespassers that access to a system is limited to authorized users. In the world of today's computer users, a password requirement is a "good fence": this amendment attempts to encourage such precautions without imposing on computer owners any requirement to implement such a precaution, and without creating any presumption that access to a system without a password requirement is authorized. Without such notice, or without actual knowledge that the access is unauthorized (i.e., accidental unauthorized access), no criminal offense should result.

The Commission believes that this amendment, or a similar amendment, would articulate clearly that mere unauthorized access to a computer or computer system, even without an intention to do further wrong, should be discouraged and punished. The amendment is designed to achieve this goal in a way that recognizes the proportionately less serious nature of the wrong, when not accompanied by a subsequent substantive crime or attempted crime. Situations in which such access is the predicate for subsequent offenses, such as the alteration of data or the theft of computer services are also dealt with in subsequent sections.

B. *Extending the vandalism prohibition to cover alteration or destruction of electronic information*

The Commission recommends the addition of the following sentence to §127 of c.266 of the Massachusetts General laws:

"The term 'personal property' as used in this section shall include, but not be limited to, electronically processed or stored data, either tangible or intangible, and data while in transit."

The existing penalties for vandalism to personal property (a penalty of the greater of \$3,000 or three times the value of the property destroyed and imprisonment for not more than 2.5 years) would also apply to computer vandalism.

Discussion of proposed amendment

The Commission is proposing here that the definition of personal property subject to prosecution for intentional alteration, damage or destruction be broadened to include electronic data. This amendment would match the earlier amendments to the larceny statute, but would not change in any way the elements of the crime or the proof to which the Commonwealth is held. The amendment simply would reflect society's commonly shared dependence upon the integrity of information that dictates human events.

This Commission is not alone in recognizing that as more and more of everyday life is managed by computers, we are compelled to ensure the integrity of the data which informs computer activity. Consider the harmful consequences of inaccurate or false information in a consumer's credit report: such consequences require that we protect against alteration, damage or destruction of information routinely managed by a computer. One need only reflect upon the many other commercial, governmental, medical, educational and public safety functions already managed by computers to recognize that the integrity of electronic data must be a social priority.

Forty-four states have enacted legislation making it a crime to alter, damage and/or destroy electronic data. Yet there is no Massachusetts statute under which a person can be prosecuted for intentionally altering, damaging or deleting another's computer information or program. In 1983, following a Supreme Judicial Court decision⁵ declaring that electronic information is not "property," the Massachusetts legislature enacted amendments to G.L. c. 266, §30, to include within the definition of "property" subject to larceny "electronically processed or stored data, either tangible or intangible, [and] data while in transit."⁶ This expansion of the definition of property, however, was limited to the crime of larceny. The legislature failed to amend G.L. c. 266, §127, which makes it a crime to destroy or injure another's property, so as to include electronic data within the purview of the property-damage law. The proposed amendment would correct this.

C. *Theft of computer services*

The Commission recommends that a new statute be passed that imposes criminal sanctions on the theft of computer service. The Commission believes that this should be limited to computer services and data that are commercially available, as opposed to private systems. As discussed below, this is in part because of the difficulty of distinguishing between different sorts of systems and services other than on the basis of commercial availability, and in part because of a belief that private system operators should exercise a greater degree of care in protecting the private nature of their systems.

The Commission suggests the following statutory language:

Commercial Computer Service fraud; penalty

"Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by any false representation, false statement, or stratagem, by unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be punished by a fine of not more than three thousand dollars or by imprisonment for not more than three years, or both. As used in this section, the words "commercial computer service" mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of data, where such use, access or copying is offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration."

⁵ Commonwealth v. Yourawski, 384 Mass.386 (1981).

⁶ Acts of 1983, c. 147 §§1 and 2.

Discussion of Proposed Amendment

In the 1960s, computer design and usage entailed physically large machines with a limited scope of functionality and applications. The machines were costly to purchase and a large amount of human effort was required to maintain very basic capabilities. Due to the high hardware costs, computers first found acceptance with government and large corporate users. For those who could afford them, they provided the service of processing large amounts of data in a shorter time.

With the advent of multi-user time sharing systems, the landscape began to change. Timesharing companies were formed. These corporations bought the large mainframe computers that small and medium size corporations could not afford and sold space and time on their computers to small and medium size firms. The service companies provided a combination of affordable access to hardware and the technical know-how to maintain specific programs required by the user. The information handled by these services remained specific to the individual subscriber. With the cost of the hardware component to the 'information system' still high, little attention was paid to the value of the information being processed.

With the introduction of the minicomputer, and then in 1982 the microcomputer or 'PC,' the cost of hardware became less of an issue. Machines became more commonplace in businesses of all sizes and in people's homes. The computer industry turned its attention towards improving the storage, manipulation, retrieval, and communication of information. Individual access to vast repositories of information on numerous subjects became a reality by the late 1980s. These technological advances also caused a decline in the costs of telecommunication. People began communicating with each other using the computer.

Within the last decade the merger of computer and communication technology has given birth to a vast assortment of electronic bulletin boards and online computer services. The typical subscriber to these services isn't interested in purchasing vast amounts of computing power (such as the original time-sharing systems offered); instead, she is interested in access--access both to other subscribers and to whatever information or services may be available through the system. Many online computer services are commercial; they charge their subscribers a fee to join the service, access the system, and perform selected services. Bulletin boards are reminiscent of telephone party lines where numerous people with common interest can talk to each other, leave messages, and obtain information or help on a specific subject. Some bulletin boards are similar to social clubs, some charge a membership fee, others are free to join but charge users who want copies of software that is made available on the system. Star Trek or Elvis fans can log onto their favorite bulletin board and talk to other fans, copy pictures or get news about conventions, etc. Users of specific computer systems can call up a bulletin board for that system and get information about new software releases or help from other users on specific problems.

Commercial online computer services offer a vast array of services to their subscribers. Prodigy allows subscribers to do their banking by computer. Dow Jones News/Retrieval provides current business and other news, and stock exchange information. CompuServe provides a shopping by computer service. Books may be read with Advantage International's Paperless Readers Club, and investment portfolios may be managed with Fidelity OnLine Express. Lexis, by Mead Data, and Westlaw, by West Publishing Company, provide lawyers with up-to-date online search and retrieval of state, federal, and specific topic legal decisions. Mead also has a news retrieval service called Nexis. And this is just a sampling of the services available to the public.

The common thread among these commercial bulletin board and online services is not as much the cost of maintaining the hardware, or the proprietary nature of the information itself (as much of the information may already be in the public domain), but the service of amassing, storing, and providing easy useful access to the information. Commercial on-line services may be more akin to department stores for information. But unlike department stores, the value of the good does not have to leave the premises for the owner to be deprived of its value. A copy of a file, the result of a search, or the displaying of stock quotations, all have value to the persons who obtain them without causing the service provider to loose control of them.

Several provisions of current Massachusetts law criminalize theft of certain types of services that are in some ways analogous to a commercial on-line computer service. These are gas and electricity, telephone and cable TV service.

The oldest of these, c.164 §126, relates to tampering with gas meters or other facilities. It derives from a statute originally passed in 1861. A similar statute, c.164 §127, dating from 1895, relates to tampering with electric meters. Although both of these statutes in their current form appear to reach theft of gas or electricity, their focus remains on the bypassing or destruction of meters or other tangible parts of the transmission system.

In 1982 the Legislature added an additional section to c.164 that squarely prohibits "unlawfully and intentionally" using or causing to be used electricity or gas without consent of the supplier or the consumer of the gas or electricity (c.164 §127A). The penalty differed significantly from that provided under the earlier statutes (a fine of not more than \$1000 or imprisonment for not more than one year, or both) in that it provided for a fine of the greater of \$1000 or triple the amount of damage, with the actual amount of damage going to the utility or customer and the excess going to the state. Damage is expressly defined to include the value of the gas or electricity used and the cost of equipment repair and replacement.

Theft of telecommunications services was apparently not a crime until 1961, when c.166 §42A was enacted. That section prohibited obtaining or attempting to obtain, with intent to defraud, telecommunications services, by false representation, unauthorized charging to the account of another by installing or tampering with equipment, "or by any other means". The penalty originally was a fine of not more than \$100 or imprisonment for not more than thirty days. This was increased in 1985 to a fine of not more than \$3000 or imprisonment for not more than three years, or both.

In 1973 c.166 §42B was enacted. This was directed specifically at devices ("blue boxes") designed, adapted or used to fraudulently obtain telecommunications services. It reached persons who made such devices, persons who sold or advertised or otherwise conveyed such devices, and persons possessing such devices with intent to use them. It also reached persons who published plans for making such devices intending that they be used to make devices to fraudulently obtain telecommunications service. This conduct originally carried a penalty of a fine of not more than \$2000 or imprisonment for not more than twelve months, or both; this was increased in 1985 to a fine of not more than \$15,000 or imprisonment for not more than four years, or both.

Responding to complaints by the emerging cable TV industry, in 1983 both §42A and §42B were amended to expressly include as "telecommunications service" the "transmission of intelligence" by cable TV companies. Consequently, the theft of cable signals in and of itself is now punishable under §42A, and the sale of unscramblers and similar devices is punishable under §42B.

This history demonstrates that there is precedent for legislation dealing with theft of computer services, and that there are effective means for dealing with problems of this nature.

It also illustrates the evolutionary process of fitting new problems into existing legal frameworks that the Commission is recommending for computer crime.

The foregoing suggestion is based upon the provisions of c.166 §42A. The Commission believes that computer services are more analogous to telecommunications services than they are to electricity or gas.

Note also that the Commission is not proposing an analog of c.166 §42B for computer services. The Commission believes that at this time such a provision would unnecessarily inhibit the development of modems and similar communications devices.

D. Modernizing the Best Evidence Rule to allow admission of duplicates of computer files

The Commission recommends the addition of the following section §79K to c.233 of the Massachusetts General laws:

Duplicates of Computer Files Admissible as Originals; Printouts of Data Files Admissible as Originals;

A duplicate of a computer data file or program file is admissible to the same extent as the original from which it is copied unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

A 'duplicate of a computer data file or program file' is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, in the normal way such a duplicate is produced on a computer, or by other equivalent techniques that accurately reproduce the original.

If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'.

Discussion of proposed amendment

The Commission recommends that the legislature and courts of Massachusetts take appropriate steps to adopt the Federal Rules of Evidence provisions regarding the definitions and admissibility of "originals" and "duplicates" of computer data. The Commission believes that modernizing Massachusetts evidence law in this way would both minimize the intrusiveness of searches and seizures of computers and increase the efficiency of criminal investigations that require the gathering of computer evidence.

As is the case in the investigations of other types of crimes, computer-crime investigations may require searches or seizures of evidence. The Fourth Amendment of the United States Constitution and Article 14 of the Massachusetts Declaration of Rights (part of the Massachusetts Constitution) require, inter alia, that such searches not be "unreasonable" and that search warrants "particularly" describe "the place to be searched, and the persons or things to be seized."

While the seizure of computer equipment should be authorized when the equipment itself is the evidence or instrumentality of a crime, in most other circumstances, where officials seek isolated information or records stored on the computer, seizure of the computer hardware normally should not be necessary, for three reasons. First, such a seizure would violate the "particularity" requirement as many non-seizable records may be seized. Second, if the warrant calls for the evidentiary search or seizure of computer-stored information or records, the seizure of the equipment itself would be beyond the scope of the warrant, absent some showing of probable cause that the equipment itself is evidence of a crime. Third, the general seizure of computer data and equipment may force a halt to legitimate business operations.

Ideally, the judicial officer should require that the search of the computer hard drive take place at the organization's premises, and that the officers executing the warrant make copies only of the seizable files or data. But this suggestion raises the concern of law-enforcement officials that a trial-court judge might, at his or her discretion, declare such copies of relevant computer data inadmissible on the grounds that the copies are not the "best evidence" of the contents of the computer at the time of the search or seizure. Such a judge would be basing his or her decision on the Best Evidence Rule (also known as "the Original Document Rule"): a rule of evidence requiring that, if a party at trial seeks to prove the contents of a document, the original of that document must be offered into evidence, unless the original is unavailable through no fault of the party seeking the admission into evidence of the copy.

The Best Evidence Rule has its roots in the common law of England in the early 18th century and, according to some commentators, it was justified in terms of the need to prevent both fraud and inaccuracy in the presentation of a document's contents as evidence.⁷ Since the typical copying methods of the 18th, 19th, and early 20th centuries posed significant risk of the introduction of inaccuracy, duplicates or copies were often ruled either inadmissible, or admissible only as "secondary evidence" of the contents of a document. To a significant extent, Massachusetts continues to follow this centuries-old, common-law rule.

Given the increasing availability of reliable copying technology, however, the trend in other American jurisdictions and in the federal courts has been to codify the Best Evidence Rule, liberalizing it to allow the admissibility of "duplicates" in place of originals, as well as a broader definition of "original." As one commentator remarks, "[t]he most reasonable accommodation of the purposes of the basic rule to modern copying to date would appear to be that of the Federal Rules of Evidence."⁸

There are three provisions of the Federal Rules of Evidence that are relevant to the admissibility of copies of computer files:

FRE 1003 provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

FRE 1001(4) provides that "[a] 'duplicate' is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, [emphasis supplied] or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

⁷ McCormick on Evidence § 231, 236 (E. W. Cleary, ed., 3d ed., 1984)

⁸ Id. at §236

FRE 1001(3) provides that "[I]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."

Taken together, these rules, if adopted by the legislature or courts of Massachusetts, provide two means for the government to prove in court the contents of computer documents without requiring the admission of the actual computer equipment on which the documents are stored. In the simplest case, a printout of a computer file, where feasible and accurate, simply would *be* an "original" for evidentiary purposes.

Where a printout would not serve, a duplicate of a computer file, following the provisions of the Federal Rules, would be just as admissible as an original (i.e., it would not be mere "secondary evidence," and the party offering the duplicate as evidence would not have to prove the unavailability of the original). According to the Advisory Committee on the 1972 Proposed Rules (which became the Federal Rules of Evidence):

When the only concern is with getting the words or other contents before the court with accuracy and precision, then a counterpart serves equally as well as the original, if the counterpart is the product of a method which insures accuracy and genuineness. By definition in Rule 1001(4), *supra*, a "duplicate" possesses this character.

Therefore, if no genuine issue exists as to authenticity and no other reason exists for requiring the original, a duplicate is admissible under the rule.⁹

Modern computer operating systems normally guarantee that a computer-produced copy of a computer file has the accuracy and genuineness required of a "duplicate" by the Federal Rules, and greater accuracy than that of photocopies, which already are frequently admitted under both the federal and the Massachusetts rules of evidence. In cases in which law-enforcement agents reasonably believe that the accurate copying of computer data by the operating system may be thwarted by a copy-protection scheme or by a software or hardware "booby-trap," the agents may employ one of several well-established procedures that allow one to bypass the operating system on the target computer and make accurate copies in spite of any countermeasures. The Commission believes Massachusetts computer equipment, software, and service vendors will gladly assist Massachusetts law-enforcement agencies in becoming familiar with these procedures.

The Commission also observes that, in addition to these substantive issues of criminal law, the consideration of "computer crime" raises new issues of procedure and policy, given the many uses to which computers are now put in the Commonwealth and elsewhere. The Commission considered whether procedural and due-process provisions might be necessary to enable law-enforcement personnel to efficiently and effectively gather evidence from a computer used for communication without unduly infringing on the First and Fourth Amendment rights of the computer owner or others. In particular, the Commission discussed the seizure of bulletin-board systems ("BBSs") and electronic mail, and how such seizures may violate the communicative rights of both targets and non-targets. Even in cases when a bulletin-board

⁹ When offered for admission in court, duplicates of computer files may be authenticated much the way other kinds of evidence in criminal cases are authenticated--that is, by testimony from those who gathered and took charge of the evidence. In addition, modern computer encryption technology holds the promise of "digital signature" and "digital timestamping" techniques that would establish beyond doubt both the accuracy of a copy and the time at which the copy was made. In the long term, Massachusetts policymakers should explore the uses and applicability of such techniques.

system or other kind of communications forum is not involved, the Commission believes, broad seizures may infringe on computer owners' privacy rights, and may interfere with the conduct of lawful activity (as when the seizure of a computer on which business records are stored prevents a lawful commercial enterprise from doing business).

However, the Commission was unable to reach a consensus on the desirability of any procedural regulations of searches and seizures. Some Commissioners expressed the opinion that there should be further study of the appropriateness of criminal-procedure reforms in cases involving the search and seizure of computer equipment or data. There may be procedural mechanisms that can limit the intrusiveness of even broad searches and seizures, for example by providing time limits on the keeping of equipment and data, and by applying "minimization" principles to the searches of stored computer data, much as they are applied to the wiretapping of telephone conversations. In his presentation before the Commission, Don Ingraham of the Alameda County District Attorney's office in Oakland, California (a nationally recognized expert in computer-crime cases) suggested to the Commission that there be procedural guarantees that would limit the extent to which law enforcement could seize and hold computer equipment and data.

Even as some Commissioners raised these concerns, other Commissioners expressed the legitimate concern of law enforcement that overly restrictive procedures would prevent the proper gathering of evidence, as in cases where seizure of the hardware on which the evidence is stored may be necessary to prevent the destruction of evidence or the obstruction of justice.

The Commission believes that civil-liberties and law-enforcement issues may converge in cases in which a broad seizure might simultaneously infringe on individual rights and create difficulties for law enforcement in sifting through large amounts of data and equipment.

Section IV

Suggestions considered and rejected by the Commission

In addition to the changes in law recommended by the Commission, the Commission considered a number of other possible legislative or policy changes. After due deliberation, the Commission has concluded specifically that none of the following changes should be made at this time. These matters are briefly discussed in this subsection.

Criminal sanctions for poor system security

There was consensus among the Commissioners that the operators of computer systems have a responsibility to take adequate precautions to guard against unauthorized access to their systems. This is particularly true for those systems containing trade secrets and other sensitive competitive and national security data and for those systems that contain sensitive data about individuals and organizations, e.g. credit-reporting agencies, hospitals, credit-card issuers, etc. Governmental authorities who maintain this sort of information have a duty to protect the privacy of their citizens. Similarly for commercial organizations, who profit from collecting and permitting access to this data.

Despite the strong consensus on the responsibility of system operators, the Commissioners rejected the suggestion that criminal sanctions be created for failure to maintain adequate security. The tools for computer security and the mores of access and conduct are

evolving too rapidly; imposing such sanctions now would threaten to severely impair the development of these industries. The Commission also notes that private causes of action exist to redress negligent and similar conduct in the maintenance of computer databases.

Treating the unauthorized copying of data as "larceny"

The Commission considered extending the reach of the general larceny statute (c.266 §30) to cover copying of all information, rather than, as under current law, only trade-secret information. The Commission believes that extending §30 to cover all information could raise serious Constitutional and policy issues. Under the U.S. Constitution, Congress alone may confer patent and copyright protection, and Congressional action in such areas preempts state law. The current federal copyright and patent statutes expressly do not preempt state trade-secret law, and such laws have been upheld by the U.S. Supreme Court. It is doubtful, however, that state legislation granting copyright-like protection to information which is not trade-secret information would survive a preemption challenge.

Furthermore, the Commission believes that an attempt to address copying of information through the larceny statute, rather than through access means, such as trespass, implicates important First Amendment issues. For a fuller discussion of the relevance of the First Amendment to computer-based communications, see Section I(C) above.

For all of these reasons, the Commission believes that the Legislature's decision to apply §30 to the copying only of trade secrets is the wisest course of action. The Commission expressly rejects extending §30 to cover copying of other data.

Theft of computer time or "clock cycles"

The Commission considered whether "theft of clock cycles"¹⁰, that is, the unauthorized use of the capabilities of a computer system, whether or not such system is offered for use generally for a fee, should be sanctioned. As described elsewhere in this report, the Commission is recommending that theft of computer service, where such service is generally available for a charge, be made criminal theft of services. Beyond that narrow change, however, the Commission concluded that theft of clock cycles should not be dealt with separately as a criminal offense.

The Commission's reasons for this conclusion include the difficulties of proving theft of cycles, the difficulties of valuation, and the somewhat nebulous concepts involved with this issue. The Commission also believes that its other recommendations will give system owners adequate protection without venturing into the ethereal realm of clock cycles.

¹⁰ Computer processors process instructions sequentially. The processor moves from one instruction to the next in a specific period of time, establishing a rhythm much like the ticking of a clock. Each tick of the processor's internal "clock" is known as a "clock cycle", and the phrase "theft of clock cycles" refers to the unauthorized use of the processor, which makes it unavailable for others to use during those cycles.

Causing the denial of computer service

Some states explicitly make it a crime to interfere with the delivery of computer service to a person or organization. The Commission believes that its recommendation with respect to theft of service legislation, combined with existing tort and other civil remedies, adequately addresses this issue.

Section V

The role of education in addressing and deterring computer crime

Education of the public through existing organizations will be a critical component of implementing effectively the legislation recommended by the Commission. Such education should be integrated into a continuum of industry standards, practices and business ethics. Education of the law enforcement community is equally essential due to the rapidity of change within the industry. Finally, expedited communication between the industry and the law enforcement community will enhance enforcement and increase sensitivity to private sector concerns. Coordination, direction, and supervision of this educational function should be committed to the Attorney General or a new special purpose body.

The fundamental role of education already has been inaugurated by creating the Commission. That role is to lay the foundation for new legislation in carefully considered, mutually recognized needs of computer users, computer vendors, law enforcement agencies and the public at large. The Commission believes it has been relatively successful in identifying such mutually recognized needs.

Following enactment of new criminal legislation several educational roles should be addressed. The primary role is that of enhancing compliance through public education. In considering this role the Commission was sensitive to the somewhat anti-authoritarian sentiment of some computer users for whom rules are to be challenged, regulations are to be resisted and systems are to be entered even if ostensibly blocked by security features.¹¹ For such users in particular, but as well for the public at large, the educational objective must be not only to disseminate the text of the law but also its rationale. This regulated community in particular must understand that the new legislation serves an important and legitimate need and that it is deliberately drafted and will be deliberately enforced so as to protect users from ill-considered, heavy-handed prosecutions.

This educational role best may be accomplished through existing educational institutions at little or no incremental cost to the Commonwealth. Public institutions and agencies would include the State Board of Education, State Board of Library Commissioners, Massachusetts Education Computer Network, University of Massachusetts and local school committees and boards. Private institutions would include the many private colleges, universities and secondary schools in the Commonwealth, Massachusetts Computer Software Council, the Massachusetts High Tech Council, the Electronic Frontier Foundation, Boston Computer Society, Massachusetts Computer-Using Educators, the EDP Auditors Association, the Massachusetts Bar Association, and the Boston Bar Association.

¹¹ See, e.g., Sterling, *The Hacker Crackdown* (1992).

The Commission also was of the view that widespread acceptance and understanding of the new legislation, and its rationale, among the user and vendor communities is essential to effective deterrence of criminal behavior. Peer pressure and common acceptance of professional standards for users and programmers can become a powerful reinforcement of the criminal law, or a significantly corrosive undermining element in achieving workplace compliance.

The development and promulgation of industry standards of professional conduct for users should be encouraged, lest the criminal law become the sole referent and guide. As in more traditional marketplaces of commerce and communication, criminal sanctions should represent the most extreme of a continuum of sanctions for unacceptable behavior, all based upon commonly accepted precepts of conduct. For example, internal control audits of data processing systems and records should derive from the same ethical standards as the criminal law and auditors and law enforcement personnel should be trained in the same curriculum, so that users may comply with common requirements.

This role of defining professional ethical standards already is at least an incidental concern of some existing industry and professional associations but, as it is the *foundation* for acceptance and compliance with legislation, it cannot itself be legislated. Coordination of the activities of such associations for this purpose should be expressly committed to a funded, stable, and nonpartisan public agency. The Commission recommends the Office of the Attorney General for this coordination role, with the admonition that the process of developing industry/user "civics" engage all the appropriate public agencies and private entities, and that it not be overly prescriptive at the expense of reflecting genuine and pragmatic marketplace expectations.

A second and major educational role recommended by the Commission is that of law enforcement agencies. Such a role is particularly important because of the rapidity of change within the computer industry. In addition to the well-recognized pace of technical innovation the industry also is characterized by quickly changing practices and expectations. Many vendors have shifted from so-called "proprietary" systems to "open" systems, that is, they have shifted from discouraging connection of third party equipment or software to encouraging such use. Likewise many vendors now publish specifications of their products which only a few years ago would have been treated as highly valuable and proprietary, in order to promote the manufacture and sale of compatible equipment and software. The capability of law enforcement agencies to remain current in this environment of rapidly changing technology and marketing practices can be enhanced greatly through appropriate educational channels into the industry through the existing industry and professional associations named above.

Finally, consistent with the rapidity of change of other elements of the industry it is the view of the Commission that many of the practices which are detrimental to the industry and appropriately would be curtailed by new legislation also are evolving rapidly; frequent communication between users and vendors on one hand and the law enforcement community on the other, will be necessary to keep the latter abreast of the latest in criminal creativity. Such need is magnified by the essentially private nature of computer crimes. Often only the victim is aware of the violation and even then the evidence may be slight; in the famous "cuckoo's egg" case the only evidence of a massive amount of illegal activity was a 75-cent discrepancy in an account.¹² Diligent reporting of evidence of illegal activity, and proper compilation of such evidence by law enforcement agencies, will be a vital tool of effective enforcement. This educational role best may be accomplished by establishing liaison roles for the industry associations (Massachusetts Computer Software Council and Massachusetts High Tech Council), working

¹² See Stoll, The Cuckoo's Egg (1989).

through the Office of the Attorney General, so that law-enforcement agencies may achieve ready access to industry expertise and information at little or no incremental cost to the Commonwealth.

In addition to enhancing prosecutions education of law enforcement agencies will assure sensitivity to the First and Fourth Amendment concerns, and privacy concerns of the public. Law-enforcement agencies will not be able to appropriately limit searches and seizures, or protect privacy interests, without a clear, current understanding of the technology and the practices of the industry. The vendors and users in the industry have an immediate and direct concern that such educational objectives are achieved and maintained. The Electronic Frontier Foundation can provide very valuable and specialized resources in this area at little incremental cost to the Commonwealth.

The Commission has not defined specific educational programs to meet the objectives summarized above. It has identified several national training programs for law enforcement agencies which are now available. It has determined that the Massachusetts Computer Software Council and the Massachusetts High Tech Council are interested in providing liaison services to the software and high tech industry in order to identify industry training and consulting resources that could be made available to the law-enforcement community. It believes that MIT, the University of Massachusetts, Harvard University and other Massachusetts institutions of higher learning, in addition to the state-wide public school system, are likely to include in their computer related curricula materials on computer crime/ethics /professionalism if such information is made available to them.

The Commission recommends that any new computer crime legislation include provisions directing the Attorney General of the Commonwealth to establish, act as liaison for, and administer educational programs that implement the foregoing purposes.



NATIONAL INSTITUTE OF JUSTICE

Research in Action

Charles B. DeWitt, Director

November 1991

State Computer Crime Statutes

by Hugh Nugent

In late 1988, Robert T. Morris, a Cornell University graduate student, shut down a nationwide computer network with what rapidly became the best known computer worm in history. Prosecuted in Federal court for violation of the Federal computer crime statute, Morris eventually received a fine and probation.¹ But his actions cut loose a torrent of public discussion on the adequacy of the criminal justice system to deal with predators as skillful as but more malicious than Morris.

Computer technology is omnipresent in contemporary American life. We pump gas from computerized pumps; receive computerized bills from public utilities for service that is largely computerized; receive computerized grocery checkout lists, which are part of computerized inventory control systems; take off, fly, and land in planes guided by computers; telephone friends on the other side of the country on computerized telecommunications systems; get telephone calls from computers; read articles, including this one, written on computers.

Hugh Nugent is an attorney and principal associate for the Institute for Law and Justice, Inc., in Alexandria, Virginia.

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Institute for Law and Justice, Inc., under contract number OJP-85-C-006.

State and Federal legislators are fully aware that we have entered the computer age. In the 10 years before the Morris worm, 48 of the 50 State legislatures and the U.S. Congress had passed some form of computer crime statute. Morris probably could have been prosecuted in every State in which his worm entered a computer, for either unauthorized access or computer damage.

When the National Institute of Justice surveyed criminal justice agencies through its National Assessment Program, police chiefs and sheriffs reported a need for more information and research on effective computer crime investigation. As part of its response, NIJ published "Dedicated Computer Crime Units," an *Issues and Practices* report

that examined special units that some jurisdictions have established specifically to investigate computer crime. As part of that study, researchers prepared an overview of State statutes on computer crimes.

This *Research in Action* summarizes the results of that effort. It examines the background and the contents of the State computer crime statutes, first with a brief discussion of some underlying issues of judicial construction and then with a review of some of the earlier computer crime cases. This background will give a better understanding of issues legislatures had in mind while drafting their computer crime statutes. The article then examines several features found in the statutes themselves, pointing out how different

From the Director

The past decade witnessed a dramatic rise in the use of computers and increasing reliance upon them throughout society. The benefits of computer technology, and its future potential, are clear. What has also become clear to the law enforcement community is the capacity of the computer as a tool for criminal activity.

Law enforcement is responding to the challenges posed by computer crime with new investigative and prosecutorial methods. The National Institute of Justice has helped with information about how agencies can implement them.

This *Research in Action* shows how State lawmakers have responded to computer crime by enacting statutes specifically targeting illegal computer activity. It summarizes some of the practical considerations that must be grappled with in responding to this criminal justice challenge.

Charles B. DeWitt
Director
National Institute of Justice

States have approached the same problems in different ways.

Strict construction of criminal statutes

The constitutional concept of due process of law, expressed in the 5th and 14th amendments of the U.S. Constitution, requires that everyone be put on clear notice that certain acts are criminal acts. This means that legislatures are to state, in terms understandable by the ordinary person, exactly what they intend to compel or prohibit. This matter of terms is one to which a great deal of attention has been paid in computer crime legislation, but anyone examining the definitions adopted would find it hard to say that they are readily understandable by the ordinary person.

A basic principle of judicial construction is that criminal statutes are strictly construed against the State and in favor of the individual. That is, courts will not interpret a statute liberally or broadly to cover the circumstances of a particular case, as they sometimes do in civil litigation, to achieve what the legislature probably had in mind but failed to express with precision and clarity. Courts will not expand criminal statutes to cover acts the legislature probably would have forbidden had it thought of them. Thus, more often than not, strict construction works for defendants in criminal cases.

Finally, a criminal offense consists of certain specific elements, all of which the prosecutor must prove. For example, larceny under common law was taking and carrying away another's personal goods of any value, with intent to steal them. That definition breaks down into four elements to be proved: (1) taking, (2) carrying away, (3) goods of another, (4) intent to deprive the owner of possession permanently. Larceny was often used as the charge against computer criminals where there was not a computer crime statute. Defenses usually raised included (1) that nothing had been "carried away," the allegedly stolen data or computer program having remained on the computer; or (2) that "property" means only "tangible property," and that

electronic impulses are not tangible. These defenses did not prevail often, but computer crime statutes focus prosecution more on the real problem and not on these tangential issues.

Computer crime cases under other criminal statutes

Computer crime was not going unpunished before the recent proliferation of computer crime statutes. Virtually every crime involving computers violates laws other than computer crime laws themselves, and prosecutors successfully prosecuted cases for embezzlement, larceny, fraud, and, in Federal courts, for wire fraud and mail fraud. But there were some problems applying older forms to newer offenses, and specifically designed computer crime statutes should alleviate these problems. Civil litigants also had been successful against computer criminals, and because most State computer crime statutes do not specifically provide for civil relief, civil litigants for the most part will continue to rely on common law or alternative statutory remedies.

Several cases collected in an *American Law Reports* annotation provide a useful background on how prosecutors proceeded before computer crime statutes were in place.² Some observations:

- Despite some ingenious defense arguments, most courts and prosecutors had little difficulty applying traditional concepts to computer offenses.
- Federal prosecutors frequently turned to wire fraud and mail fraud charges where State prosecutors would have charged fraud, larceny, or embezzlement.
- Courts sometimes refused to apply traditional definitions to new offenses where there was no readily apparent loss by the victim.

Defenses usually rested on the intangible or incorporeal nature of computer transactions. In a Texas case, the defendant stole 59 computer programs and attempted to sell them to one of his employer's clients for \$5 million. One of his defenses was that computer programs are not corporeal property and therefore not subject to theft. The court noted that the

Texas Penal Code section under which the case was brought defines "property," as related to the crime of theft, as including "all writings of every description, provided such property possesses any ascertainable value." It had no trouble finding that computer programs fall within the meaning of that provision.³ The Alabama Supreme Court reached much the same conclusion in a civil case involving theft of computer payroll programs.⁴

The "intangibility" argument was also unavailing for a Federal defendant charged with unauthorized use of property of the United States. He had accessed a NASA computer from his home telephone, using its time and storage capacity for his own business. He argued that computer time and storage capacity are not "property" or "a thing of value" within the meaning of the statute under which he was prosecuted, characterizing them as "mere philosophical concepts as distinguished from interests capable of being construed as property." The court rejected the argument:

The consumption of its time and the utilization of its capacities seem to the court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be questioned. Thus, the uses of the computer and the product of such uses would appear to the court to be a "thing of value" within the meaning of 18 USC §641, sufficient upon which to predicate a legally sufficient indictment.⁵

A Missouri defendant tried a variation on the intangibility argument.⁶ He was charged with stealing by deceit after he used another person's automatic teller card to withdraw \$800 in 16 transactions of \$50 each over a 9-day period. Defendant argued that the indictment failed to state that he had made any representation at all, let alone a fraudulent representation, and failed to state that the bank had acted in reliance on his representations in parting with the \$800. The court rejected this argument, saying it was based on the assumption that the misrepresentation had to have been verbal. Actions suffice, and by his actions defendant represented that he had authority to use the other

person's bank card and code. The court stated:

Just as the facts here show a misrepresentation by defendant through his conduct, so also the facts clearly show reliance thereon by the bank. The machine was so programmed that no money would be paid out without the insertion of the appropriate card and the corresponding personal identification numbers. When those items were supplied, the response was programmed so as to pay out the money. No difference can be perceived whether the bank gave approval after the presentation of those identification items or whether it programmed its acceptance in advance. In either case, the bank equally relied upon the presentation of the card and personal identification.⁷

Several cases illustrate the ease with which Federal prosecutors turn computer crime into wire fraud or mail fraud. For example, two TWA employees in Pittsburgh worked a fraud on TWA by keeping and then voiding one-way tickets that had been paid for in cash. They would give the travelers boarding passes and credit transaction receipts, which few people would even notice, let alone question. The two kept the actual ticket, reassembled the ticket packet, and sent it to auditing to be canceled. Of course, they kept the cash. Part of this transaction entailed printing the ticket, which was done by computer connected to the TWA mainframe in Kansas City. It was this part of the transaction that turned the matter into a Federal wire fraud, of which the two were convicted.⁸

In another case, a retail merchant in Brooklyn used counterfeit credit cards to defraud VISA and MasterCard on 267 spurious purchases worth over \$95,000. Because computerized inquiries to the credit card companies were made on interstate telephone lines, he was found guilty of wire fraud.⁹

A third Federal case was a mail fraud case in which the mailing was a relatively minor part of the offense, which in all other respects was clearly a computer crime. While working for Sperry Univac's applications development center,

defendants developed a system which used computers to generate sheet music. In doing so, they used substantial amounts of computer time and storage capacity within the central processing unit of the applications center development, all without Sperry Univac's knowledge or authorization. In collaboration with another corporation, they agreed to develop and market their sheet music system. The other corporation sent promotional materials through the mail, supplying the basis for the mail fraud prosecution.¹⁰

There are three cases where lack of a computer crime statute defeated prosecution. *Lund v. Commonwealth*¹¹ led directly to enactment of Virginia's computer crime statute. It is a good example of a court's refusal to stretch old concepts to fit new offenses. Lund was a graduate student in statistics at Virginia Tech who used the university's computer time and services to work on his doctoral thesis, charging the costs back to various departments. He was prosecuted for grand larceny and larceny by false pretense. The Supreme Court of Virginia reversed his conviction. Strictly construing Virginia's larceny statutes, the court held that computer time and services were not goods and chattels (personal property) within the meaning of the statutes, and they could not be carried away. The Virginia General Assembly responded first by amending the larceny statute to include computer time or services,¹² later by enacting a comprehensive computer crime statute.¹³

In *People v. Weg*,¹⁴ defendant was a computer programmer for the New York City Board of Education. He was accused of using the board's computer system to record and retrieve data for his own commercial benefit. More specifically, he was charged with theft of services under New York Penal Code §165.15(8), which reads:

Obtaining or having control...of business, commercial or industrial equipment or facilities of another person, knowing that he is not entitled to the use thereof, and with intent to deprive a commercial or other substantial benefit for himself or a third person, he uses or diverts to the use of himself

or a third person such labor, equipment or facilities.

The court held that the board of education's computer was not "business" equipment, since both the statutory context and legislative history clearly indicated that the legislature had meant to protect equipment in commercial use. The board's computer service was not rented or sold to outsiders for a fee.

The court went on to point out that if the legislature wanted to make unauthorized use of computers a crime, it could do so, as Illinois had done:

This Court, however, may not create an offense. Unless Penal Law section 165.15(8) is amended, it will apply only to unauthorized tapping into a computer whose service is for hire.¹⁵

Finally, in *State v. McGraw*,¹⁶ McGraw worked for the city of Indianapolis as a computer operator. The city leased computer services on a fixed charge or flat rate basis, so its costs did not vary with the amount of use. McGraw was provided a terminal at his desk and was assigned a portion of the computer's information storage area, called a "private library," for his use in performing his duties.

McGraw became involved in a private sales venture and began soliciting his fellow employees and using a small portion of his assigned library to maintain records. Reprimanded several times for selling his products in the office and on office time, he was eventually fired. After he was fired, McGraw asked a former fellow employee to obtain a printout of his business data and then to erase it from what had been his library. Instead, the printout was turned over to McGraw's former supervisor and became the basis for the criminal charges against him.

McGraw was charged with theft, in that he knowingly exerted "unauthorized control over the property of the City of Indianapolis, Indiana, to wit: the use of computers and computer services with intent to deprive the City of Indianapolis..." The Indiana Supreme Court reversed McGraw's conviction because

an element of the offense was missing. The court assumed that McGraw's use of the computer was unauthorized and that such use was "property" under the theft statute. But there was still the question of "deprivation." The quote is presented at length because of the down-to-earth analogies used by the defendant and the court:

...Our question is, "Who was deprived of what?"

Not only was there no evidence that the City was ever deprived of any part of the value or the use of the computer by reason of Defendant's conduct, the uncontradicted evidence was to the contrary. The computer was utilized for City business by means of terminals assigned to various employee-operators, including Defendant. The computer processed the data from the various terminals simultaneously, and the limit of its capacity was never reached or likely to have been. The computer service was leased to the City at a fixed charge, and the tapes or discs upon which the imparted data was stored were erasable and reusable. Defendant's unauthorized use cost the City nothing and did not interfere with its use by others. He extracted from the system only such information as he had previously put into it. He did not, for his own benefit, withdraw City data intended for its exclusive use or for sale. Thus, Defendant did not deprive the City of the "use of computers and computer services" as the information alleged that he intended to do. We find no distinction between Defendant's use of the City's computer and the use, by a mechanic, of the employer's hammer or a stenographer's use of the employer's typewriter for other than the employer's purpose. Under traditional concepts, the transgression is in the nature of a trespass, a civil matter—and a de minimis one, at that. Defendant has likened his conduct to the use of an employer's empty bookshelf, for the temporary storage of one's personal items, and to the use of an employer's telephone facilities for toll-free calls. The analogies appear to us to be appropriate.¹⁷

One judge dissented, disagreeing with the majority's conclusion that McGraw did not intend to deprive the city of any property.

Time and use are at the very core of the value of a computer system. To say that only the information stored in the computer plus the tapes and discs and perhaps the machinery involved in the computer system, are the only elements that can be measured as the value or the property feature of that system, is incorrect.

The fact is the City owned the computer system and all the stations including the defendant's. The time and use of that equipment at that station belonged to the City.¹⁸

The *Lund*, *Weg*, and *McGraw* cases would all have had different outcomes under computer crime statutes. The court in *Weg* expressly said that the New York Legislature could make computer abuse a crime if it chose to, but that it had not so chosen. The Virginia Legislature reacted to *Lund* in exactly that way, enacting a computer crime statute.

There is another common thread in these three cases. The courts could well have been resisting imposition of severe penalties in cases where victims had not in fact suffered demonstrable monetary loss. In the discussion of computer crime statutes that follows, access without harm is criminalized, although penalties for simple access are usually not harsh.

Computer crime statutes

The first State computer crime statute was enacted in Florida in 1978. It became effective on August 1, 1978, and Arizona's statute took effect 2 months later. Other States soon followed, with 49 now having adopted some form or other of computer crime law. West Virginia and Maine are the most recent, in 1989 and 1990. As this article is being prepared for publication, Massachusetts is in the final stages of enacting a comprehensive computer crime statute, replacing what had been a reference to "electronically stored data" in its general larceny stat-

ute.¹⁹ Only Vermont has not enacted specific computer crime provisions.

Except in Virginia, it was not unsuccessful prosecutions under traditional criminal statutes that stimulated this legislative activity. It is hard to say what did, aside from widespread publicity about potential problems. A very interesting analysis of the history of this legislation can be found in an article by Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws."²⁰

Most States that have addressed the issue of computer crime have done so in a comprehensive statute, often an independent title in the State criminal code called the Computer Crime Act.²¹ At the other extreme, Ohio has inserted a series of computer crime definitions in its general theft statute and added one section on denying access to a computer.²²

As mentioned above, most States have created a separate code section for computer crime, but many have placed it in other categories such as crimes against property, fraud, theft, or business and commercial offenses. Arizona has placed its computer crime provisions under organized crime and fraud, and North Dakota under racketeer-influenced and corrupt organizations (RICO).

The differences between freestanding computer crime statutes and amendments to existing criminal codes should not be overstated. Some of the former are very brief, targeting computer problems, such as unauthorized access or damage to a computer, and leaving other crimes involving computers to be covered by the criminal code as before.²³ On the other hand, California's computer crime provisions, which appear under crimes against property, are quite comprehensive.²⁴

There is a philosophical difference between the two approaches that deserves comment.²⁵ With the comprehensive approach, the State legislature creates a new set of definitions and offenses, trying to face the broad array of potential criminal opportunities created by com-

puter technology. There is always a fear that new definitions will give rise to new litigation as courts and litigants shake them down into accepted forms.

The other philosophy is to modify existing law by incorporating new concepts within established forms, thereby minimizing the potential for frustrating the legislative will. Established statutory definitions, approved jury instructions, and judicial precedents can be used. For example, if computer crime is viewed as a form of property crime, then the familiar concepts of property crime can be used in developing and defending cases. The impact of change is alleviated.

Although there is no universally recognized model for computer crime statutes, many provisions appear with only slight changes in several States. The typical computer crime statute will contain the following elements:

- Definitions of terms.
- Offenses.
- Elements of offenses.
- Penalties.

Some statutes contain additional provisions:

- Venue.
- Civil remedies.
- Affirmative defenses.

[A compilation of State computer crime statutes as of June 30, 1990, is available on loan from the National Criminal Justice Reference Service (NCJRS), Box 6000, Rockville, MD 20850. Phone 800-851-3420; in Maryland and the Washington, D.C., metropolitan area phone 301-251-5500. Refer to NCJ 127854 when requesting this information from NCJRS.]

Definitions of terms

The definitions set forth in these statutes are always a clear indicator of what problems the legislature is attempting to address. Typically, the following terms will be defined:

- Access.
- Computer.
- Computer network.
- Computer program.
- Computer software.
- Computer system.
- Data.
- Financial instrument.
- Property.

All of the above terms are defined in at least 20 State statutes, and most in over

Definitions Used in the Tennessee Code

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means a device that can perform substantial computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job;

(3) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them;

(4) "Computer program" means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data;

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network;

(6) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(7) "Data" is a representation of information, knowledge, facts, concepts, or instructions that are being

prepared or have been prepared in a formalized manner, and are intended to be stored or processed, or are being stored or processed, or have been stored or processed, in a computer, computer system, or computer network;

(8) "Financial instruments" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, or marketable security, or any computer system representation thereof;

(9) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(10) "To process" is to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result;

(11) "Property" includes, but is not limited to, intellectual property, financial instruments, data, computer programs, documentation associated with data, computers, computer systems and computer programs, all in machine-readable or human-readable form, and any tangible or intangible item of value; and

(12) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer programs, or data to perform tasks.

30. At the other extreme are several terms that appear in only one or two statutes:

- Computer control language (Maryland).
- Computer data base (Maryland).
- Computer hacking (South Carolina).
- Computer supplies (Wisconsin).
- Data base (New Jersey, Pennsylvania).
- Private personal data (Connecticut, Delaware).
- Supporting documentation (Wisconsin).

These definitions are generally an interesting combination of legal and computer technical styles. Lawyerly words and phrases abound: "including but not limited to," "and any other," "or otherwise," "tangible or intangible," "representation." Computer terms are represented by words like "input," "output," "software," "data base," "supporting documentation," "computer network," "computer system."

To illustrate what State legislatures have been doing with definitions, set forth in the accompanying sidebar are Tennessee's definitions, which are typical.²⁶

Several other definitions are of particular interest. For example, according to South Carolina:²⁷

(j) "Computer hacking" means accessing all or part of a computer, computer system, or a computer network for the purpose of establishing contact only without the intent to defraud or commit any other crime after such contact is established and without the use of computer-related services except such services as may be incidental to establishing contact.

In a parallel provision, South Carolina makes computer hacking a computer crime in the third degree, a misdemeanor with a maximum \$200 fine and 30 days jail for the first offense, but a felony with a maximum \$2,000 fine and 2 years for the second offense.²⁸ California has a

similar provision, but it increases the fine to \$5,000 for a second hacking offense.²⁹

In its first computer crime statute, Illinois defined "electronic bulletin board" and "identification codes/password systems,"³⁰ but those terms disappeared in a 1987 revision in favor of the terms most frequently seen in the codes of other States, such as "access," "computer," "computer program," and "data."³¹

Offenses

State statutes do not always give computer offenses specific names and they use a variety of descriptions to state exactly what they are prohibiting. Among the most frequently used titles or descriptions of offenses are the following:

- Access To Defraud.
- Access To Obtain Money.
- Computer Fraud.
- Offenses Against Computer Users.
- Offenses Against Intellectual Property.
- Offenses Against Computer Equipment and Supplies.
- Unauthorized Access.
- Unauthorized or Unlawful Computer Use.

Defining access offenses is a legislative means of applying common law trespass concepts to computers. In other words, an access offense is usually entering someone else's property. If there is no criminal intent beyond curiosity or mischief, then the offense is like South Carolina's definition of computer hacking. But if there is criminal intent, usually to commit a fraud or theft of some kind, then the perpetrator can be prosecuted for both the unauthorized access and the other crime.

There are further wrinkles to access provisions. It is usually specified that interfering with someone else's legitimate access is an offense. Defendants often start out with a right to access, and some States provide for an affirmative defense of authorization, or at least a reasonable belief that access was author-

ized. Virginia, in a section protecting privacy, draws a line between authorized and unauthorized access, a line that might be easily crossed in an authorized user's search of a data base:

A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.³²

Unauthorized access is like trespass. Unauthorized taking of computer programs or data is like theft of any other property. In New York, possession of stolen computer programs or data is, in one sense, like possession of any other stolen property, but, in another sense, like possession of a stolen key or a combination to a safe. Unlawful duplication of computer-related material is a felony. Possession of such material, with the intention to benefit someone other than the owner, is a separate felony.³³

Elements of computer crimes

State legislatures have drafted their statutes in very similar, although not identical, ways, so a few examples will suffice to show what specific elements they have included in computer crimes. Virginia provides a compact example of a statute that covers many points in four relatively short sections:³⁴

§ 18.2-152.3. Computer Fraud.

Any person who uses a computer or computer network without authority and with the intent to: (1) Obtain property or services by false pretenses; (2) Embezzle or commit larceny; or (3) Convert the property of another shall be guilty of the crime of computer fraud...

§ 18.2-152.4. Computer Trespass.

Any person who uses a computer or

computer network without authority and with the intent to: (1) Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network; (2) Cause a computer to malfunction regardless of how long the malfunction persists; (3) Alter or erase any computer data, computer programs or computer software; (4) Effect the creation or alteration of a financial instrument or of an electronic transfer of funds; (5) Cause physical injury to the property of another; or (6) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network shall be guilty of the crime of computer trespass...

§ 18.2-152.6. **Theft of Computer Services.** Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services...

§ 18.2-152.7. **Personal Trespass by Computer.** A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.

(Another portion of the Virginia statute, Invasion of Privacy, appears in the previous section.³⁵)

Virginia uses the term "use" where most other States would say "access." Tennessee provides a typical example of how legislatures have specified the elements of access offenses:³⁶

(a) Whoever knowingly and willfully, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations,

or promises violates this subsection and is subject to the penalties of Section 39-14-105.

(b) Whoever intentionally and without authorization, directly or indirectly

- (1) Accesses, or
- (2) Alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network, or computer software, program or data violates this subsection.

(e) Whoever receives, conceals, or uses, or aids another in receiving, concealing or using any proceeds resulting from a violation of either subsection (a) or (b)(2) of this section, knowing same to be the proceeds of such violation, or whoever receives, conceals, or uses, or aids another in receiving, concealing or using, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing same to have been used in violating either subsection (a) or (b)(2) of this section violates this subsection and shall be subject to the penalties of Section 39-14-105.

Wisconsin exemplifies another approach, that of focusing completely on the computer without reference to intent to commit some other crime:³⁷

(2) Offenses against computer data and programs.

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies data, computer programs or supporting documentation.
2. Destroys data, computer programs or supporting documentation.
3. Accesses data, computer programs or supporting documentation.
4. Takes possession of data, computer programs or supporting documentation.
5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(3) Offenses against computers, computer equipment or supplies.

(a) Whoever willfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b):

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.
2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

A widely publicized computer crime case, *State of Texas v. Burleson*,³⁸ was brought under the Texas provision on harmful access. Three weeks before he was fired by an insurance agency, Burleson had created a logic bomb in the company's systems that would periodically destroy records. Three days after he was fired, the company's computer system suffered a major loss of records, over 160,000 records in three different files.³⁹ He was tried and convicted under the harmful access section, which reads as follows:⁴⁰

Harmful access

(a) A person commits an offense if the person intentionally or knowingly:

- (1) causes a computer to malfunction or interrupts the operation of a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer; or
- (2) alters, damages, or destroys data or a computer program stored or maintained, or produced by a computer, without the effective consent of the owner or licensee of the data or computer program.

Penalties

Sanctions provided in State computer crime statutes fall roughly into three classes, each of them used by about a third of the States. The overall sanction system of a State's criminal code is of great importance. A third of the States group all sanctions in a separate part of the code, working towards uniformity in sentencing through a systematic classification of crimes and sanctions. In these States, computer crimes will be classified as Class A Felonies, Class B Felonies, Class C Felonies, Class A Misdemeanors, etc. In such States, the range of penalties and fines will not appear in the computer crime statute itself.

In another third of the States, the penalties are explicitly stated in the computer crime statute. The ranges of fines and sentences are set forth and tied directly to the offenses defined by the statute. Under both these systems, States are penalizing computer crimes at both felony and misdemeanor level. In most States, the maximum penalties will be 5 years and \$25,000, but in Nevada, the fine can be \$100,000 and the sentence 6 years, and in South Carolina, the fine can be \$125,000 and the sentence 10 years.

The third class of computer crime penalties takes a different, and sometimes problematic, approach. It ties the penalty to the amount of damage or loss suffered by the victim. New Mexico sets five levels of sanctions for computer fraud, computer abuse, and unauthorized computer use, depending on the value of the money, property, or services lost:

- Less than \$100, petty misdemeanor.
- Between \$100 and \$250, misdemeanor.
- Between \$250 and \$2,500, fourth degree felony.
- Between \$2,500 and \$20,000, third degree felony.
- More than \$20,000, second degree felony.⁴¹

However, such damages are often difficult to measure. Computer services and computer time are bought and sold daily, so arriving at their value should not be

difficult. But for proprietary computer uses that are not sold as such, assessing value gets more complex. In a case involving theft of seismic computer programs used in the petroleum industry, an expert witness testified that these programs were worth more than \$50, the statutory minimum required to be proved in the case. He also testified that these programs were worth perhaps as much as \$2 1/2 million.⁴² The statutory minimum obviously had no relationship to the true value of the programs.

In *State of Texas v. Burleson*,⁴³ the insurance company whose records Burleson had destroyed offered evidence on what it cost to replace and rehabilitate those records.

Connecticut and Delaware empower the court, in lieu of imposing a fine, to sentence the defendant to pay an amount not to exceed double the amount of defendant's gain from the offense. The court may hold a separate hearing on that issue if there is insufficient evidence in the record upon which to base a finding of the defendant's gain.⁴⁴ Montana sets the ceiling on a fine at two and one-half times the value of the property used, altered, destroyed, or obtained.⁴⁵

Illinois and California have stringent forfeiture provisions, enabling courts to deprive offenders of the instrumentalities of their crimes.⁴⁶ The Illinois statute also reaches the fruits or proceeds of the crime.

Wisconsin empowers a sentencing judge, in addition to other penalties, to place restrictions on the offender's use of computers. The duration of such a restriction may not exceed the length of time to which the offender could have been sentenced.⁴⁷

Wisconsin is also one of the States that makes special provision for offenses that create "unreasonable risk and high probability of death or great bodily harm to another," making such offenses Class C felonies.⁴⁸ Virginia makes "personal trespass by computer," that is, unauthorized use with intent to cause physical injury, a Class 3 felony.⁴⁹

Delaware classifies offenses creating "a risk of serious physical injury to another" as Class C felonies.⁵⁰

Florida makes offenses against computer equipment or supplies a felony of the second degree "if there is an interruption or impairment of governmental operation or public communication, transportation or supply of water, gas, or other public service..."⁵¹

Venue

A dozen States include specific venue provisions in their computer crime statutes. Venue refers to the place, that is, the judicial district, in which a case can be prosecuted, which for most crimes is the place where the crime was committed. Venue questions have arisen in computer crime cases because the perpetrator can be at a place quite remote from the place, or places, at which his offense has impact. In a case in which defendants had rigged the Pennsylvania lottery, the offense had impact everywhere in the State where there was a terminal connected to the lottery (1,400 in all). Some of the defendants challenged their prosecution in Harrisburg, claiming that none of the acts that were the basis for the charges had taken place there. The court found from the evidence that the lottery's central computer, without which the rigging could not have taken place, was in Harrisburg and therefore that the offense was committed there.⁵²

Venue statutes deal with these problems by making offenses prosecutable in any one of several places. Georgia and Virginia have added provisions pertaining to the computer owner's principal place of business. Georgia's venue provision reads as follows:⁵³

For the purpose of venue under this article, any violation of this article shall be considered to have been committed:

- (1) In any county in which any act was performed in furtherance of any transaction which violated this article;
- (2) In the county of the principal place of business in this State of the owner or

lessee of a computer, computer system, computer network, or any part thereof:

(3) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, or other material or objects which were used in furtherance of the violation: and

(4) In any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication.

Civil remedies

Computer crime statutes routinely provide that they are not meant to limit any other provision of civil or criminal codes, leaving the State free to prosecute offenders on other statutory bases, such as fraud or embezzlement, and leaving victims free to pursue their ordinary civil remedies, such as fraud or conversion. Because the level of proof in civil litigation is not as high, and because statutory and common law civil remedies can be broadly construed and shaped to accord relief, there is not the same sense of urgency about providing specific statutory civil remedies for computer crime. But several States have provided such remedies, and it is interesting to note what they have added.

California and Missouri provide compensatory damages, "including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access."⁵⁴ The same section of the California Penal Code also provides that "the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor."

Other than the compensatory damage language quoted in the preceding paragraph, civil remedy provisions of computer crime statutes do not say much

about how the plaintiff's damages are to be measured. Virginia, however, provides that: "Without limiting the generality of the term, 'damages' shall include loss of profits."⁵⁵

Delaware and Wisconsin provide for injunctions against computer offenses as part of their civil remedies. Wisconsin's statute adds protection against bulletin board activity or other disclosure of confidential passwords or codes:

In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.⁵⁶

California, Illinois, Missouri, and New Jersey provide for attorneys' fees. New Jersey allows the award of punitive damages. Delaware has what amounts to a civil forfeiture provision.⁵⁷

Miscellaneous features

In addition to features common to the majority of computer crime statutes, there are several that appear in only one or two States, but are worth noting. For example, North Carolina has an explicit provision covering extortion:

Any person who verbally or by a written or printed communication, maliciously threatens to commit an act described in G.S. 14-455 [Damaging computers and related materials] with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a Class H felony.⁵⁸

Georgia and Utah create a statutory duty to report computer crimes to law enforcement officials. Georgia's is the more elaborate of the two:

It is the duty of every business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corpo-

ration; or other business entity which has reasonable grounds to believe that a violation of this article has been committed to report promptly the suspected violation to law enforcement authorities. When acting in good faith, such business; partnership; college; university; person; state, county, or local governmental agency or department or branch thereof; corporation; or other business entity shall be immune from any civil liability for such reporting.⁵⁹

Neither Georgia nor Utah provides any sanction for failure to report. It is not clear that these acts create any greater obligation than citizens already have to report crimes.

Washington makes explicit what is left implicit in most other places:

A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.⁶⁰

To the extent that other States address this issue, they do so by providing that computer crime provisions are not exclusive and that all other parts of the State code still apply.

In addition to prohibiting unauthorized access to a computer, computer system, or computer network for illicit purposes, Utah makes it a separate offense to allow another person to do the same acts.⁶¹ Iowa addresses a problem about which most other States remain silent, that of proving what is in a computer. The following provision makes printouts admissible as evidence:

In a prosecution under this chapter, computer printouts shall be admitted as evidence of any computer software, program, or data contained in or taken from a computer, notwithstanding an applicable rule of evidence to the contrary.⁶²

The rule of evidence to the contrary would be the "best evidence rule," that the best evidence of the content of a document is the document itself. Iowa's

statute eliminates any contention that the printout is only a copy of what is in the computer, not the data that are really there. Best evidence rule arguments have been made in earlier cases.⁶³

Virginia and West Virginia specifically provide that a computer can be used as an instrument of forgery,⁶⁴ legislatively resolving a definitional problem that had vexed at least two Federal courts.⁶⁵

One final note. Oklahoma's statute, reflecting one of that State's principal concerns, includes "geophysical data or the interpretation of that data" in its definition of "property."⁶⁶

Computer worms and viruses

The beginning of this article referred to the computer worm used by Robert Morris to penetrate a national network. Even though most States already had computer crime statutes, several State legislatures amended their statutes to include detailed descriptions of Morris' techniques.

The Morris worm was an independent program that penetrated computers on the network and replicated itself, rapidly overloading the individual computers, first making them sluggish and then causing them to crash. The worm created temporary files that disappeared when the affected computers were shut down, and it did not steal information or destroy files. In the jargon of the industry, because Morris' program was an independent program, it was a "worm." A computer "virus" is a piece of computer code attached to another program.

California's amendment, which refers to both worms and viruses under the rubric "computer contaminant," is illustrative of the new provisions adopted after the Morris incident.⁶⁷

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.

They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

Maine and Texas both added "computer virus" to their definitions,⁶⁸ and Minnesota added "destructive computer program" to its definitions.⁶⁹ Illinois put its new prohibition under "computer tampering."⁷⁰

Conclusion

Justice Holmes considered the States laboratories for working out a variety of approaches to problems confronting our society. The computer crime statutes just discussed are an excellent example of what he was talking about. In a very short period of time, short, that is, as far as lawmaking goes, almost all States have adopted legislation dealing directly and explicitly with computer crime. They have chosen to add these statutes to existing law, rather than to substitute them for prior criminal prohibitions and civil remedies, broadening the options available to prosecutors and civil litigants.

These laws are detailed in definition and comprehensive in scope. But if anything characterizes the criminals at whom these laws are aimed, it is their own ingenuity in finding cracks and loopholes in computer systems and networks. The next decade will provide a test of the strength and precision of these computer laws.

Endnotes

1. Morris was prosecuted under 18 U.S.C. §1030. See *New York Times*, Sec. 1, p. 1, May 5, 1990; *Washington Post*, p. A-1, May 5, 1990, for full discussions of Morris' offense and sentence. An excellent discussion of the Morris worm, its impact, and the prosecutorial issues can be found in Harold L. Burstyn, "RTM

and the Worm That Ate Internet," *Harvard Magazine*, p. 23, May-June 1990.

2. *State v. McGraw*, 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985), ANNOTATION: Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 A.L.R.4th 971. This is a collection of cases that have been published in case reporting systems, primarily the regional reporters of the West Publishing Company. There undoubtedly have been many other cases, including prosecutions under computer crime statutes, in which there was no reported opinion of the court. E.g., the Robert Morris case is unreported, Morris having pled guilty and there being no written opinion by the court.

3. *Hancock v. State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).

4. *National Surety Corp. v. Applied Systems*, 418 So.2d 847 (Ala. 1982).

5. *United States v. Sampson*, 6 Comp.L.Serv.Rep. 879 (N.D.Cal. 1978).

6. *State v. Hamm*, 569 S.W.2d 289 (Mo.App. 1978).

7. 569 S.W.2d at 291 (Mo.App. 1978).

8. *United States v. Giovengo*, 637 F.2d 941 (3d Cir. 1980), cert. den., 450 U.S. 1032, 101 S.Ct. 1743, 68 L.Ed.2d 228.

9. *United States v. Muni*, 668 F.2d 87 (2d Cir. 1981).

10. *United States v. Kelly*, 507 F.Supp. 495 (E.D.Pa. 1981).

11. 217 Va. 688, 232 S.E.2d 745 (1977).

12. See *Evans v. Commonwealth*, 226 Va. 292, 308 S.E.2d 126 (1983).

13. Va. Code §§18.2-152.1 through 18.2-152.14.

14. 113 Misc.2d 1017, 450 N.Y.S.2d 957 (N.Y.City Crim. Ct. 1982).

15. 450 N.Y.S.2d at 961.

16. 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985).

17. 480 N.E.2d at 554.
18. 480 N.E.2d at 555.
19. M.G.L.A. c. 266, §30(2).
20. *Criminology*, 26:101, 1988.
21. E.g., see Alabama Computer Crime Act, Ala. Code §§13-A-8-100 through 103; Florida Computer Crimes Act, Fla. Stat. §§815.01 through 815.07; Illinois Computer Crime Prevention Law, Ill. Rev. Stat., ch. 38, §§16D-1 through 16D-7.
22. Ohio Rev. Code Ann. §§2901.01, 2913.81.
23. E.g., see Ala. Code §§102, 103; Ky. Rev. Stat. §§434.840 through 434.860.
24. Cal. Penal Code. §§502, 502.01; see also §§1203.047, 2702.
25. This point was emphasized to the author by a senior deputy prosecuting attorney from the State of Washington, who participated in writing his State's computer crime provisions, which he referred to as one of the "modification" statutes.
26. Tenn. Code §39-14-601.
27. S.C. Code §16-16-10 (j).
28. S.C. Code §16-16-20 (4).
29. Cal. Penal Code §502 (d)(3)(A), (B).
30. Ill. Rev. Stat., c. 38, §16-9, repealed, P.A. 85-926, eff. Dec.1,1987.
31. Ill. Rev. Stat., ch. 38, §16D-2.
32. Va. Code §18.2-152.5, A.
33. N.Y. Penal Code §§156.30, 156.35.
34. Va. Code §§18.2-152-3, 152-4, 152-6, and 152.7.
35. Va. Code §18.2-152.5. See text at note 32, *supra*.
36. Tenn. Code §39-14-602.
37. Wis. Stat. §943.70.
38. No. 0274120R, Tarrant County, Texas, Criminal Court, 1988.
39. For a discussion of the Burleson case and its investigation, see J. Thomas McEwen, "Dedicated Computer Crime Units," *NIJ Issues and Practices*, 1989.
40. Tex. Penal Code §33.03.
41. N.M. Stat. 30-45-3, 30-45-4, 30-45-5.
42. *Hancock v. State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. 1966).
43. See text at note 38, *supra*.
44. 1984 Conn. Gen. Stat. Ann. §53a-257; Del. Code Ann. Title 11, §937 (f).
45. Mont. Code Ann. §45-6-311 (c)(2).
46. Ill. Rev. Stat., ch. 38, §16D-6; Cal. Penal Code, §502 (g), 502.01.
47. Wis. Stat. §943.70 (4).
48. Wis. Stat. §943.70 (2)(b)(4), (3)(b)(4).
49. Va. Code §18.2-152.7.
50. Del. Code Ann. Title 11, §937 (c).
51. Fla. Stat. §815.05 (2)(b)(3).
52. *Com. v. Katsafanas*, 464 A.2d 1270 (Pa. Super. 1983).
53. Ga. Code §16-9-94.
54. California Penal Code §502 (e)(1); Missouri Code §537.525 is almost identical in its wording.
55. Va. Code §18.2-152.12.
56. Wis. Code §943.70 (5).
57. Del. Code Title 11, §939 (a).
58. N.C. Gen. Stat. §14-457.
59. Ga. Code §16-9-95. Cf. Utah Code §76-6-705.
60. Wash. Rev. Ann. Code §9A.52.130.
61. Utah Code Ann. §76-6-703 (3).
62. Iowa Code Ann. §716A.16.
63. See *Hancock v. State*, 402 S.W.2d 906, 18 A.L.R.3d 1113 (Tex. Crim. App. 1966).
64. Va. Code §18.2-152.14; W.Va. Code §61-3C-15.
65. *United States v. Jones*, 553 F.2d 351 (4th Cir. 1977), cert. den., 431 U.S. 968, 97 S.Ct. 2928, 53 L.Ed.2d 1064.
66. Okla. Stat. Ann. §1952 (8).
67. Ca. Penal Code §502 (b)(10).
68. MRSA §431 (9); Tex. Penal Code §33.01 (9).
69. Minn. Stat. §609.87. Subd. 12.
70. Ill. Rev. Stat. Ch. 38, §16D-3 (4).

	Use without authority	Alter	Damage	Destroy	Block Use	Copy Files	Disclose Information	Takes	Use for Crime	Takes Possession
Alabama	X			X			X	X	X	
Alaska		X	X					X		
Arizona		X	X	X						
Arkansas	X	X	X						X	
California	X	X	X	X	X				X	
Colorado	X	X	X	X	X				X	
Connecticut	X	X	X	X						
Delaware	X	X	X	X	X		X	X		
Florida		X		X	X		X	X	X	
Georgia		X	X	X			X	X	X	
Hawaii		X	X	X			X	X	X	
Idaho	X	X	X	X					X	
Illinois	X	X	X	X					X	
Indiana	X	X	X						X	
Iowa	X		X	X					X	
Kansas	X	X	X	X		X	X			
Kentucky	X	X	X	X					X	
Louisiana	X	X		X		X	X	X		
Maine	X									
Maryland	X									
Massachusetts								X		
Michigan		X	X	X					X	
Minnesota			X	X				X	X	
Mississippi		X	X	X	X	X	X	X	X	
Missouri		X		X	X		X	X	X	
Montana	X	X		X					X	
Nebraska	X	X	X	X	X		X			
Nevada	X	X		X	X		X	X		
New Hampshire	X	X	X	X	X	X	X	X		
New Jersey	X	X	X	X		X		X		
New Mexico	X	X	X	X				X	X	
New York	X	X		X					X	
North Carolina	X	X	X	X	X				X	
North Dakota	X	X	X	X	X	X	X	X	X	
Ohio	X	X	X	X	X	X	X	X	X	
Oklahoma		X	X	X		X			X	
Oregon	X	X	X	X					X	
Pennsylvania		X	X	X	X				X	
Rhode Island		X	X	X				X		
South Carolina		X	X	X					X	
South Dakota	X	X		X					X	
Tennessee	X	X	X	X					X	
Texas	X	X	X	X	X				X	
Utah		X	X	X	X					
Vermont										
Virginia	X	X		X	X	X		X	X	
Washington	X							X	X	
West Virginia	X	X	X	X					X	
Wisconsin	X	X	X	X		X	X			X
Wyoming	X		X	X	X					

State	Citations	Added or modified provisions since 1988
Alabama	Code 13A-8-101	
Alaska	Stat. §§ 11.81.900 (b) (44) & 11.46.200 (a)	
Arizona	Rev. St. §§ 13-2301E &13-2316	
Arkansas	Code §§ 5-41-102 through 5-41-106	
California	Penal Code §§ 502 &484j	
Colorado	Rev. St. §18-5.5-101	
Connecticut	Gen. St. §53a-250	
Delaware	Code tit. 11, §931 to 939	
Florida	St. §815.01	
Georgia	Code §16-9-90	
Hawaii	Rev. St. 708-890	
Idaho	Code §18-22	
Illinois	St. ch. 38, para 16D	Insertion of computer virus that will damage or destroy a computer or data or harm users; and "aggravated computer virus insertion" which disrupts functioning of state or local government or public utility or causes bodily harm
Indiana	Code §35-43-1-2 through 4	
Iowa	Code §716A	
Kansas	§21-3755	
Kentucky	Rev. St. §434-840	
Louisiana	Rev. St. 14:73.1 to 5	
Maine	Rev. St. tit. 17A §431	New statute. Unauthorized invasion of computer system, including copying, damaging, or introducing a virus
Maryland	Code Art. 27 §146	
Massachusetts	MGL ch.266 §30(2)	
Michigan	Comp. Laws §752.791	
Minnesota	St. §§ 609.87 & 609.89	Insertion of computer virus; theft by computer; unauthorized access
Mississippi	Code §97-45-1	
Missouri	St. § 569.093	
Montana	Code 45-6-310	
Nebraska	Rev. St. §28-1343	
Nevada	Rev. St. §205.473	
New Hampshire	Rev. St. §638:16	
New Jersey	Rev. St. §§2A:38A-1 (civ) & 2C:20-1 (criminal)	

State	Citations	Added or modified provisions since 1988
New Mexico	St. § 30-16A-1	
New York	Pen.Law para.156	
North Carolina	Gen.St. 14-453	
North Dakota	Cent.Code §12.1-06.1-08	
Ohio	Rev.Code §§2901.01 & 2913.01	
Oklahoma	St. tit. 21, §§ 1951-1956	
Oregon	Rev.St. 164.377	
Pennsylvania	St. tit. 18, § 3933	
Rhode Island	G.L. § 11-52-1	
South Carolina	Code §16-16-10	
South Dakota	Codified L. §43-43B-7	
Tennessee	Code §39-14-60	Apparently renumbered from §39-3-1404; no other obvious changes.
Texas	Penal Code §33.01 & Civ.St. Art. 5429b	
Utah	Code §76-6-701	
Virginia	Code §18.2-152.1	
Washington	Rev.Code §9A.48.100	
West Virginia	Code §61-3c-4 through 12	New statute. Fraud, tampering, and unauthorized access.
Wisconsin	St. §943.70	
Wyoming	St. §6-3-501 through 504	
Federal	18 USC 1030, 40 USC 759	

Appendix C

18 USC 1030 FEDERAL COMPUTER FRAUD AND ABUSE STATUTE

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer,

(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer; shall be punished as provided in subsection (c) of this section.

(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

(A) causes loss to one or more others of a value aggregating \$1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another

offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "federal interest computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States. (Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190, and amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065 Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(aX5), Aug. 9, 1989 103 Stat. 502-Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925.) (e)(4)(H), is classified to section 310i of Title 12, Banks and Banking. Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (section 601 et seq.) of chapter 6 of Title 12. Section 25(a) of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter II (section 611 et seq.) of chapter 6 of Title 12. Separability of Provisions. If any provision of Pub.L. 101-73 or the application thereof to any person or circumstance is held invalid, the remainder of Pub.L. 101-73 and the application of the provision to other persons not similarly situated or to other circumstances not to be affected thereby, see section 1221 of Pub.L. 101-73, set out as a note under section 1811 of Title 12, Banks and Banking.

Reports of Prosecutions. Section 2103 of Pub.L. 98-473, Oct. 12, 1984, 98 Stat. 2192, provided: "The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution [Oct. 12, 1984], concerning prosecutions under the sections of title 18 of the United States Code added by this chapter."

Appendix D

California Computer Crime Statute (1980)

§ 502. [Definitions: Computer Crimes: Status as felonies: Construction of section.]

(a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specific functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Services" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representation, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

(d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

(e) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction. [1798 ch 858 § 1]

California Penal Code § 502. (1992)

§ 502. Computer crimes

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(d)

(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars (\$ 10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$ 5,000), or by imprisonment in

the county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation which does not result in injury, and where the value of the computer services used does not exceed four hundred dollars (\$ 400), by a fine not exceeding five thousand dollars (\$ 5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$ 5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars (\$ 400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars (\$ 10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (8) of subdivision (c) is punishable as follows:

(A) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars (\$ 250).

(B) For any violation which results in a victim expenditure in an amount not greater than five thousand dollars (\$ 5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars (\$ 5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation which results in a victim expenditure in an amount greater than five thousand dollars (\$ 5,000), by a fine not exceeding ten thousand dollars (\$ 10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars (\$ 5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(e)

(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that

effect.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)

(1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of supplies and computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed an accumulated total of one hundred dollars (\$100).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

New Mexico Statutes on Computer-related Crime
N.M. Stat. Ann. 30-45-1 to 30-45-7 (1992)

30-45-1. Short title

This act [30-45-1 to 30-45-7 NMSA 1978] may be cited as the "Computer Crimes Act".

30-45-2. Definitions

As used in the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978]:

A. "access" means to program, execute programs on, intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any computer resources, including data or programs of a computer, computer system, computer network or database;

B. "computer" includes an electronic, magnetic, optical or other high-speed data processing device or system performing logical, arithmetic or storage functions and includes any property, data storage facility or communications facility directly related to or operating in conjunction with such device or system. The term does not include an automated typewriter or typesetter or a single display machine in and of itself, designed and used solely within itself for word processing, or a portable hand-held calculator, or any other device which might contain components similar to those in computers but in which the components have the sole function of controlling the device for the single purpose for which the device is intended;

C. "computer network" means the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers;

D. "computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from a computer system;

E. "computer property" includes a financial instrument, data, databases, computer software, computer programs, documents associated with computer systems and computer programs, or copies, whether tangible or intangible, and data while in transit;

F. "computer service" includes computer time, the use of the computer system, computer network, computer programs or data prepared for computer use, data contained within a computer network and data processing and other functions performed, in whole or in part, by the use of computers, computer systems, computer networks or computer software;

G. "computer software" means a set of computer programs, procedures and associated documentation concerned with the operation and function of a computer system;

H. "computer system" means a set of related or interconnected computer equipment, devices and software;

I. "data" means a representation of information, knowledge, facts, concepts or instructions which are prepared and are intended for use in a computer, computer system or computer network;

J. "database" means any data or other information classified, processed, transmitted, received, retrieved, originated, switched, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer system, computer network or computer software; and

K. "financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction, authorization mechanism, marketable security or any other computerized representation thereof.

30-45-3. Computer access with intent to defraud or embezzle

Any person who knowingly and willfully accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to obtain, by means of embezzlement or false or fraudulent pretenses, representations or promises, money, property or anything of value, where:

A. the money, property or other thing has a value of one hundred dollars (\$100) or less is guilty of a petty misdemeanor;

B. the money, property or other thing has a value of more than one hundred dollars (\$100) but not more than two hundred fifty dollars (\$250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

C. the money, property or other thing has a value of more than two hundred fifty dollars (\$250) but not more than two thousand five hundred dollars (\$2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

D. the money, property or other thing has a value of more than two thousand five hundred dollars (\$2,500) but not more than twenty thousand dollars (\$20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

E. the money, property or other thing has a value of more than twenty thousand dollars (\$20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-4. Computer abuse

Any person who knowingly, willfully and without authorization, or having obtained authorization:

A. directly or indirectly alters, changes, damages, disrupts or destroys any computer, computer network, computer property, computer service or computer system where:

(1) the damage to the computer property or computer service has a value of one hundred dollars (\$100) or less is guilty of a petty misdemeanor;

(2) the damage to the computer property or computer service has a value of more than one hundred dollars (\$100) but not more than two hundred fifty dollars (\$250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

(3) the damage to the computer property or computer service has a value of more than two hundred fifty dollars (\$250) but not more than two thousand five hundred dollars (\$2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

(4) the damage to the computer property or computer service has a value of more than two thousand five hundred dollars (\$2,500) but not more than twenty thousand dollars (\$20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

(5) the damage to the computer property or computer service has a value of more than twenty thousand dollars (\$20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

B. directly or indirectly introduces or causes to be introduced data which the person knows to be false into a computer, computer system, computer network, computer software, computer program, database or any part thereof with the intent of harming the property or financial interests or rights of any person is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-5. Unauthorized computer use

Any person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity such authorization provides for purposes to which the authorization does not extend, directly or indirectly accesses, uses, takes, transfers, conceals, obtains, copies, or retains possession of any computer, computer network, computer property, computer service, computer system or any part thereof where:

A. the damage to the computer property or computer service has a value of one hundred dollars (\$100) or less is guilty of a petty misdemeanor;

B. the damage to the computer property or computer service has a value of more than one hundred dollars (\$100) but not more than two hundred fifty dollars (\$250) is guilty of a misdemeanor and shall be sentenced pursuant to the provisions of Section 31-19-1 NMSA 1978;

C. the damage to the computer property or computer service has a value of more than two hundred fifty dollars (\$250) but not more than two thousand five hundred dollars (\$2,500) is guilty of a fourth degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978;

D. the damage to the computer property or computer service has a value of more than two thousand five hundred dollars (\$2,500) but not more than twenty thousand dollars (\$20,000) is guilty of a third degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978; or

E. the damage to the computer property or computer service has a value of more than twenty thousand dollars (\$20,000) is guilty of a second degree felony and shall be sentenced pursuant to the provisions of Section 31-18-15 NMSA 1978.

30-45-6. Prosecution

A. Prosecution pursuant to the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978] shall not prevent any prosecutions pursuant to any other provisions of the law where such conduct also constitutes a violation of that other provision.

B. A person found guilty of violating any provision of the Computer Crimes Act shall, in addition to any other punishment, be ordered to make restitution for any financial loss sustained by anyone injured as the direct result of the commission of the crime. Restitution shall be imposed in addition to incarceration, forfeiture or fine, and not in lieu thereof, and may be

made a condition of probation. The defendant's present and future ability to make such restitution shall be considered. In an extraordinary case, the court may determine that the interests of those injured and justice would not be served by ordering restitution. In such a case, the court shall make and enter specific written findings on the record substantiating the extraordinary circumstance presented upon which the court determined not to order restitution. In all other cases, the court shall determine the amount and method of restitution.

30-45-7. Forfeiture of property

A. The following are subject to forfeiture:

- (1)all computer property, equipment or products of any kind which have been used, manufactured, acquired or distributed in violation of the Computer Crimes Act [30-45-1 to 30-45-7 NMSA 1978];
- (2)all materials, products and equipment of any kind which are used or intended for use in manufacturing, using, accessing, altering, disrupting, copying, concealing, destroying, transferring, delivering, importing or exporting any computer property or computer service in violation of the Computer Crimes Act;
- (3)all books, records and research products and materials involving formulas, microfilm, tapes and data which are used or intended for use in violation of the Computer Crimes Act;
- (4)all conveyances, including aircraft, vehicles or vessels, which are used or intended for use to transport or in any manner to facilitate the transportation of property described in Subsection A, B or C of this section for the purpose of violating the Computer Crimes Act;
- (5)all property, real, personal or mixed, which has been used or intended for use, maintained or acquired in violation of the Computer Crimes Act; and
- (6)all money or proceeds that constitute an instrumentality or derive from a violation of the Computer Crimes Act.

B. Notwithstanding the provisions of Paragraphs (1) through (6) of Subsection A of this section:

- (1)no conveyance used by any person as a common carrier in the transaction of business as a common carrier is subject to forfeiture under this section unless it appears that the owner or other person in charge of the conveyance is a consenting party to a violation of the Computer Crimes Act;
- (2)no conveyance, computer property, equipment or other material is subject to forfeiture under this section by reason of any act or omission established by the owner to have been committed or omitted without his knowledge or consent;
- (3)a conveyance, computer property, equipment or other material is not subject to forfeiture for a violation of law the penalty for which is a misdemeanor or petty misdemeanor; and

(4)a forfeiture of a conveyance, computer property, equipment or material encumbered by a bona fide security interest shall be subject to the interest of a secured party if the secured party neither had knowledge of nor consented to the act or omission.

C. Property subject to forfeiture and disposal under the Computer Crimes Act may be seized by any law enforcement officer upon an order issued by the district court having jurisdiction.

D. Seizure without such an order may be made if:

(1)the seizure is incident to an arrest or search under a search warrant;

(2)the property subject to seizure had been the subject of a prior judgment in favor of the state in an injunction or forfeiture proceeding based upon the Computer Crimes Act; or

(3)the enforcement officer has probable cause to believe that the property, whether real, personal or mixed, was used or intended for use, maintained or acquired in violation of the Computer Crimes Act.

E. In the event of a seizure pursuant to Subsection C or Subsection D of this section, a proceeding under the Computer Crimes Act and the rules of civil procedure for the district courts shall be instituted promptly and not later than thirty days after seizure. The proceeding to forfeit property under the Computer Crimes Act is against the property and not against the owner or any other person. It is in rem wholly and not in personam. It is a civil case and not a criminal proceeding. The forfeiture proceeding is required, not to complete the forfeiture, but to prove the illegal use for which the forfeiture was suffered.

F. Except as otherwise specifically provided by law, whenever any property is forfeited to the state by reason of the violation of any law, the court by which the offender is convicted shall order the sale or other disposition of the property and the proceeds of any such sale as provided for in this section are subject to the court making due provisions for the rights of innocent persons and the legitimate rights to restitution on behalf of actual victims of the criminal acts.

G. Property taken or detained under this section shall not be subject to replevin but is deemed to be in the custody of the law enforcement agency seizing it subject only to the orders and decrees of the district court. When property is seized under the Computer Crimes Act, the enforcement officer may:

(1)place the property under seal;

(2)remove the property to a place designated by the law enforcement officer or by the district court; or

(3)require the law enforcement agency to take custody of the property and remove it to an appropriate location for disposition in accordance with law.

H. When property is forfeited under the Computer Crimes Act, the law enforcement agency seizing it shall:

(1)deliver custody of the property to the information systems council attached to the general services department. The council, based upon a plan, shall advertise and make available the forfeited property to stated agencies and political subdivisions of the state based upon a demonstrated need and plan of use for that property. The

information systems council shall advertise and make the forfeited property available by bid for a minimum of one hundred twenty days and dispose of that property within another sixty days. All proceeds from the sale of forfeited property shall be deposited in the general fund; or

(2) where the court orders the property to be sold, the proceeds of the sale shall be paid into the general fund.

Appendix E

EXCERPTS FROM OHIO COMPUTER CRIME STATUTES OHIO REVISED CODE

§ 2901.01 DEFINITIONS

As used in the Revised Code:

- (A) "Force" means any violence, compulsion, or constraint physically exerted by any means upon or against a person or thing.
- (D) "Physical harm to property" means any tangible or intangible damage to property which, in any degree, results in loss to its value or interferes with its use or enjoyment. "Physical harm to property" does not include wear and tear occasioned by normal use.
- ...
- F) "Serious physical harm to property" means any physical harm to property which does either of the following:
- ...
- (1) Results in substantial loss to the value of the property, or requires a substantial amount of time, effort, or money to repair or replace;
- (2) Temporarily prevents the use or enjoyment of the property, or substantially interferes with its use or enjoyment for an extended period of time.
- ...
- (J) (1) "Property" means any property, real or personal, tangible or intangible, and any interest or license in such property. "Property" includes, but is not limited to, cable television service, computer data, computer software, financial instruments associated with computers, and other documents associated with computers, or copies of the documents, whether in machine or human readable form. "Financial instruments associated with computers" include, but are not limited to, checks, drafts, warrants, money orders, notes of indebtedness, certificates of deposit, letters of credit, bills of credit or debit cards, financial transaction authorization mechanisms, marketable securities, or any computer system representations of any of them.
- (2) As used in this division and division (M) of this section, "cable television service," "computer," "computer software," "computer system," "computer network," and "data" have the same meaning as in section 2913.01 of the Revised Code.
- ...
- (M) "Contraband" means any property described in the following categories:
- ...
- (7) Any equipment, machine, device, apparatus, vehicle, vessel, container, liquid, or substance that has been, is being, or is intended to be used in an attempt or conspiracy to violate, or in the violation of, any law of this state relating to alcohol or tobacco;

- (8) Any personal property that has been, is being, or is intended to be used in an attempt or conspiracy to commit, or in the commission of, any offense or in the transportation of the fruits of any offense;

...

- (10) Any computer, computer system, computer network, or computer software that is used in a conspiracy to commit, an attempt to commit, or in the commission of any offense, if the owner of the computer, computer system, computer network, or computer software is convicted of or pleads guilty to the offense in which it is used.

§ 2901.12 VENUE

...

- I. (1) When the offense involves a computer, computer system, or computer network, the offender may be tried in any jurisdiction containing any location of the computer, computer system, or computer network of the victim of the offense or any jurisdiction in which the alleged offender commits any activity that is an essential part of the offense.
- (2) As used in this section, "computer," "computer system," and "computer network" have the same meaning as in section 2913.01 of the Revised Code.

§ 2913.01 DEFINITIONS

As used in this chapter:

...

- (E) "Services" include labor, personal services, professional services, public utility services, common carrier services, and food, drink, transportation, entertainment, and cable television services.
- (F) "Writing" means any computer software, document, letter, memorandum, note, paper, plate, data, film, or other thing having in or upon it any written, typewritten, or printed matter, and also means any token, stamp, seal, credit card, badge, trademark, label, or other symbol of value, right, privilege, license, or identification.
- ...
- (L) "Computer services" includes, but is not limited to, the use of a computer system, computer network, computer program, data that is prepared for computer use, or data that is contained within a computer system or computer network.
- (M) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses. "Computer" includes, but is not limited to, all input, output, processing, storage, computer program, or communication facilities that are connected, or related, in a computer system or network to such an electronic device.
- (N) "Computer system" means a computer and related devices, whether connected or unconnected, including, but not limited to, data input, output, and storage devices, data communications links, and computer programs and data that make the system capable of

performing specified special purpose data processing tasks.

- (O) "Computer network" means a set of related and remotely connected computers and communication facilities that includes more than one computer system that has the capability to transmit among the connected computers and communication facilities through the use of computer facilities.
- (P) "Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, cause the computer to process data.
- (Q) "Computer software" means computer programs, procedures, and other documentation associated with the operation of a computer system.
- (R) "Data" means a representation of information, knowledge, facts, concepts, or instructions that are being or have been prepared in a formalized manner and that are intended for use in a computer system or computer network. For purposes of section 2913.47 of the Revised Code, "data" has the additional meaning set forth in division (A) of that section.
- (S) "Cable television service" means any services provided by or through the facilities of any cable television system or other similar closed circuit coaxial cable communications system, or any microwave or similar transmission service used in connection with any cable television system or other similar closed circuit coaxial cable communications system.
- (T) "Gain access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

§ 2913.04 UNAUTHORIZED USE OF PROPERTY: UNAUTHORIZED ACCESS TO COMPUTER SYSTEM

- (A) No person shall knowingly use or operate the property of another without the consent of the owner or person authorized to give consent.
- (B) No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, or computer network without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, or computer network or other person authorized to give consent by the owner.
- (C) The affirmative defenses contained in division (C) of section 2913.03 of the Revised Code are affirmative defenses to a charge under this section.
- (D) Whoever violates this section is guilty of unauthorized use of property. If the offense involves a violation of division (A) of this section and does not involve any computer, computer system, computer network, computer software, or data, unauthorized use of property is a misdemeanor of the fourth degree. If the offense involves a violation of division (A) of this section and involves any computer, computer system, computer network, computer software, or data or if the offense involves a violation of division (B) of this section, unauthorized use of property is whichever of the following is applicable:
 - (1) If division (D)(2) or (3) of this section does not apply, a felony of the fourth

degree;

- (2) If division (D)(3) of this section does not apply and the offender previously has been convicted of a theft offense, a felony of the third degree;
- (3) If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, a felony of the second degree.

§ 2913.42 TAMPERING WITH RECORDS

(A) No person, knowing he has no privilege to do so, and with purpose to defraud or knowing that he is facilitating a fraud, shall do any of the following:

- (1) Falsify, destroy, remove, conceal, alter, deface, or mutilate any writing, data, or record;
- (2) Utter any writing or record, knowing it to have been tampered with as provided in division (A)(1) of this section.

(B) No person, knowing he has no privilege to do so, shall falsify, destroy, remove, conceal, alter, deface, or mutilate any computer software or data.

- (C) (1) Whoever violates this section is guilty of tampering with records.
- (2) If the offense involves a violation of division (A) of this section and does not involve data, tampering with records is whichever of the following is applicable:
 - (a) If division (C)(2)(b) of this section does not apply, a misdemeanor of the first degree;
 - (b) If the writing or record is a will unrevoked at the time of the offense or a record kept by or belonging to a governmental agency, a felony of the fourth degree.
- (3) If the offense involves a violation of division (A) of this section involving data, tampering with records is whichever of the following is applicable:
 - (a) If division (C)(3)(b) or (c) of this section does not apply, a felony of the fourth degree;
 - (b) If division (C)(3)(c) of this section does not apply and the writing or record is a record kept by or belonging to a governmental agency or the offender previously has been convicted of a theft offense, a felony of the third degree;
 - (c) If the value of the data involved in the offense or the loss to the victim is one hundred dollars or more, a felony of the second degree.

- (4) If the offense involves a violation of division (B) of this section, tampering with records is whichever of the following is applicable:
- (a) If division (C)(4)(b) or (c) of this section does not apply, a felony of the fourth degree;
 - (b) If division (C)(4)(c) of this section does not apply and the offender previously has been convicted of a theft offense, a felony of the third degree;
 - (c) If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, a felony of the second degree.

§ 2913.81 DENYING ACCESS TO A COMPUTER

- (A) No person, without privilege to do so, shall knowingly deny or cause the denial of a computer system or computer services to an authorized user of a computer system or computer services that, in whole or in part, are owned by, under contract to, operated for, or operated in conjunction with another person.
- (B) Whoever violates this section is guilty of denying access to a computer, a felony of the fourth degree. If the offender previously has been convicted of a theft offense, denying access to a computer is a felony of the third degree. If the offense is committed for the purpose of devising or executing a scheme to defraud or to obtain property or services and the value of the property or services or the loss to the victim is one hundred thousand dollars or more, denying access to a computer is a felony of the second degree.

